(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004 年4 月1 日 (01.04.2004)

PCT

(10) 国際公開番号
WO 2004/028072 A1

(51) 国際特許分類[7]: H04L 9/08, 9/10, 9/32, G09C 1/00

(21) 国際出願番号: PCT/JP2003/011804

(22) 国際出願日: 2003 年9 月17 日 (17.09.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2002-273444 2002 年9 月19 日 (19.09.2002) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 Tokyo (JP).

(72) 発明者; および

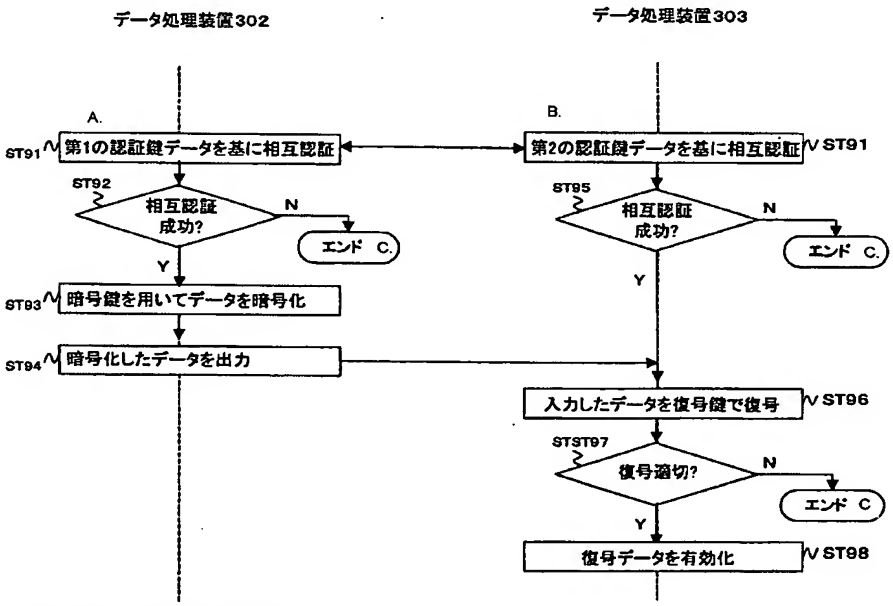
(75) 発明者/出願人 (米国についてのみ): 大森 和雄 (OMORI,Kazuo) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP). 本城 哲 (HONJO,Akira) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP). 末吉 正弘 (SUEYOSHI,Masahiro) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP). 花木 直文 (HANAKI,Naofumi) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP). 舘野 啓 (TATENO,Kei) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP).

(74) 代理人: 佐藤 隆久 (SATOH,Takahisa); 〒111-0052 東京都 台東区 柳橋２丁目４番２号 宮木ビル４階 創進国際特許事務所 Tokyo (JP).

[続葉有]

(54) Title: DATA PROCESSING METHOD, ITS PROGRAM, AND ITS DEVICE

(54) 発明の名称: データ処理方法、そのプログラムおよびその装置



302...DATA PROCESSING DEVICE
303...DATA PROCESSING DEVICE
A...PERFORM TWO-WAY AUTHENTICATION USING FIRST AUTHENTICATION KEY DATA SET.
B...PERFORM TWO-WAY AUTHENTICATION USING SECOND AUTHENTICATION KEY DATA SET.
ST92...TWO-WAY AUTHENTICATION SUCCESSFUL?
C...END
ST93...ENCRYPT DATA USING ENCRYPTION KEY.
ST94...OUTPUT ENCRYPTED DATA.
ST96...DECRYPT RECEIVED DATA USING DECRYPTION KEY.
STST97...DECRYPTION SUCCESSFUL?
ST98...VALIDATE DECRYPTED DATA.
ST95...TWO-WAY AUTHENTICATION SUCCESSFUL?

(57) Abstract: Data processing devices (302, 303) authenticates each other using first and second authentication key data sets (ST91). If the two-way authentication is successful, the data processing device (302) encrypts predetermined data using encryption key data and outputs the encrypted data to the data processing device (303) (ST93, ST94). The data processing device (303) decrypts the encrypted data using decryption key data (ST96), judges if the decryption is successful, and validates the data (ST97, ST98)

(57) 要約: データ処理装置３０２と３０３との間で第１および第２の認証鍵データを用いて相互認証を行う（ＳＴ９１）。当該相互認証が成功すると、データ処理装置３０２が所定のデータを暗号鍵データを用いて暗号化してデータ処理装置３０３に出力する（ＳＴ９３，ＳＴ９４）。データ処理装置３０３は、復号鍵データを用いて上記暗号化データを復号し（ＳＴ９６）、それが適切か否かを判断して有効化する（ＳＴ９７，ＳＴ９８）。

WO 2004/028072 A1

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明　細　書

データ処理方法、そのプログラムおよびその装置

技術分野

本発明は、認証結果を基に所定の処理を行うデータ処理方法、そのプログラムおよびその装置に関する。

背景技術

第１のデータ処理装置と第２のデータ処理装置との間で相互認証を行い、お互いの正当性を認証した後に、第１のデータ処理装置から第２のデータ処理装置に暗号化したデータを出力するシステムがある。

このようなシステムでは、上記相互認証と上記データの暗号化とで同じ鍵データを用いている。

しかしながら、上述した従来のシステムのように、上記相互認証と上記データの暗号化とで同じ鍵データを用いると、相互認証の鍵データが第三者によって不正に取得された場合に、伝送される暗号化データも当該鍵データを用いて不正に解読されてしまうという問題がある。

発明の開示

本発明はかかる事情に鑑みてなされたものであり、認証の鍵データが不正に第三者によって取得された場合でも、認証に続いて提供された暗号化データがその第三者によって解読されないようにすることを可能にするデータ処理方法、そのプログラムおよびその装置を提供することを目的とする。

上述した目的を達成するために、第１の発明のデータ処理方法は、第１のデータ処理装置が第１の認証鍵データおよび暗号鍵データを保持し、第２のデータ処

理装置が前記第１の認証鍵データに対応した第２の認証鍵データと前記暗号鍵データに対応した復号鍵データとを保持する場合に、前記第１のデータ処理装置と前記第２のデータ処理装置とが行うデータ処理方法であって、前記第１のデータ処理装置が前記第１の認証鍵データを用い、前記第２のデータ処理装置が前記第２の認証鍵データを用いて、前記第１のデータ処理装置と前記第２のデータ処理装置との間で認証を行う第１の工程と、前記第２のデータ処理装置が、前記第１の工程の前記認証により前記第１のデータ処理装置の正当性を認めた場合に、前記第１のデータ処理装置が前記暗号鍵データを用いて暗号化を行って前記第２のデータ処理装置に提供した暗号化データを、前記復号鍵データを用いて復号する第２の工程と、前記第２のデータ処理装置が、前記第２の工程の前記復号によって得た復号データが適切に復号されたものであると判断した場合に、前記復号データを有効なものとして用いる第３の工程とを有する。

第１の発明のデータ処理方法の作用は以下のようになる。

第１の工程において、第１のデータ処理装置が第１の認証鍵データを用い、第２のデータ処理装置が第２の認証鍵データを用いて、前記第１のデータ処理装置と前記第２のデータ処理装置との間で認証を行う。

そして、第２の工程において、前記第２のデータ処理装置が、前記第１の工程の前記認証により前記第１のデータ処理装置の正当性を認めた場合に、前記第１のデータ処理装置が前記暗号鍵データを用いて暗号化を行って前記第２のデータ処理装置に提供した暗号化データを、前記復号鍵データを用いて復号する。

そして、第３の工程において、前記第２のデータ処理装置が、前記第２の工程の前記復号によって得た復号データが適切に復号されたものであると判断した場合に、前記復号データを有効なものとして用いる。

第１の発明のデータ処理方法は、好ましくは、前記第１の工程において、前記第１のデータ処理装置および前記第２のデータ処理装置が、第１の暗号化アルゴリズム並びに前記第１の暗号化アルゴリズムに対応した第１の復号アルゴリズム

を基に、所定のデータの暗号化および復号を行って前記認証を行い、前記第２の工程において、前記第２のデータ処理装置が、第２の暗号化アルゴリムを基に暗号化された前記暗号化データを、前記第２の暗号化アルゴリズムに対応した第２の復号アルゴリズムを基に前記復号する。

また、第１の発明のデータ処理方法は、好ましくは、前記第１の認証鍵データが所定の鍵データを用いて所定の生成方法で生成されている場合に、前記第１の工程は、前記第１のデータ処理装置が、前記第１の認証鍵データの生成に用いられた鍵データを指定する鍵指定データを前記第２のデータ処理装置に提供する第４の工程と、前記第２のデータ処理装置が、前記第４の工程で受けた前記鍵指定データが指定する前記鍵データを用いて前記所定の生成手法で前記第２の認証鍵データを生成する第５の工程と、前記第１のデータ処理装置が前記第１の認証鍵データを用い、前記第２のデータ処理装置が前記第５の工程で生成した前記第２の認証鍵データを用いて、前記認証を行う第６の工程と、前記第２のデータ処理装置が、前記第６の工程の前記認証により、前記第１の認証鍵データと前記第２の認証鍵データとが同じであると判断すると、前記第１のデータ処理装置の正当性を認める第７の工程とを有する。

第２の発明のデータ処理システムは、第１の認証鍵データおよび暗号鍵データを保持する第１のデータ処理装置と、前記第１の認証鍵データに対応した第２の認証鍵データと前記暗号鍵データに対応した復号鍵データとを保持する第２のデータ処理装置とを有し、前記第１のデータ処理装置が、前記第１の認証鍵データを用い、前記第２のデータ処理装置が前記第２の認証鍵データを用いて、前記第１のデータ処理装置と前記第２のデータ処理装置との間で認証を行い、前記第２のデータ処理装置が、前記認証により前記第１のデータ処理装置の正当性を認めた場合に、前記第１のデータ処理装置が前記暗号鍵データを用いて暗号化を行って前記第２のデータ処理装置に提供した暗号化データを、前記復号鍵データを用いて復号し、前記第２のデータ処理装置が、前記復号によって得た復号データが

適切に復号されたものであると判断した場合に、前記復号データを有効なものとして用いる。

第２の発明のデータ処理システムの作用は以下のようになる。

第１のデータ処理装置が、第１の認証鍵データを用い、第２のデータ処理装置が前記第２の認証鍵データを用いて、第１のデータ処理装置と前記第２のデータ処理装置との間で認証を行う。

そして、前記第２のデータ処理装置が、前記認証により前記第１のデータ処理装置の正当性を認めた場合に、前記第１のデータ処理装置が前記暗号鍵データを用いて暗号化を行って前記第２のデータ処理装置に提供した暗号化データを、前記復号鍵データを用いて復号する。

そして、前記第２のデータ処理装置が、前記復号によって得た復号データが適切に復号されたものであると判断した場合に、前記復号データを有効なものとして用いる。

第３の発明のデータ処理方法は、認証鍵データおよび暗号鍵データを保持するデータ処理装置が行うデータ処理方法であって、前記認証鍵データを用いて、認証先と認証を行う第１の工程と、前記第１の工程の前記認証の後に、前記暗号鍵データを用いて所定のデータを暗号化する第２の工程と、前記第２の工程の前記暗号化により得られたデータを前記認証先に出力する第３の工程とを有する。

第４の発明のデータ処理装置は、所定のデータを暗号化して認証先に出力するデータ処理装置であって、認証鍵データおよび暗号鍵データを記憶する記憶手段と、前記認証鍵データを用いて、認証先と認証を行う認証手段と、前記認証手段の前記認証の後に、前記暗号鍵データを用いて所定のデータを暗号化する暗号化手段と、前記暗号化手段の前記暗号化により得られたデータを前記認証先に出力する出力手段とを有する。

第５の発明のプログラムは、認証鍵データおよび暗号鍵データを保持するデータ処理装置が実行するプログラムであって、前記認証鍵データを用いて、認証先

と認証を行う第１の手順と、前記第１の手順の前記認証の後に、前記暗号鍵データを用いて所定のデータを暗号化する第２の手順と、前記第２の手順の前記暗号化により得られたデータを前記認証先に出力する第３の手順とを有する。

第６の発明のデータ処理方法は、認証鍵データおよび復号鍵データを保持するデータ処理装置が行うデータ処理方法であって、前記認証鍵データを用いて、被認証手段と認証を行う第１の工程と、前記復号鍵データを用いて、前記被認証手段から受けたデータを復号する第２の工程と、前記第１の工程の前記認証により前記被認証手段の正当性を認めると、前記第２の工程の前記復号により得られたデータを有効なものとして用いる第３の工程とを有する。

第７の発明のデータ処理装置は、認証鍵データおよび復号鍵データを保持するデータ処理装置であって、前記認証鍵データを用いて、被認証手段と認証を行う認証手段と、前記被認証手段からデータを入力する入力手段と、前記復号鍵データを用いて、前記入力手段を介して前記被認証手段から入力した前記データを復号する復号手段と、前記認証手段の前記認証により前記被認証手段の正当性を認めると、前記復号手段の前記復号により得られたデータを有効なものとして用いる制御手段とを有する。

第８の発明のプログラムは、認証鍵データおよび復号鍵データを保持するデータ処理装置が実行するプログラムであって、前記認証鍵データを用いて、被認証手段と認証を行う第１の手順と、前記復号鍵データを用いて、前記被認証手段から受けたデータを復号する第２の手順と、前記第１の手順の前記認証により前記被認証手段の正当性を認めると、前記第２の手順の前記復号により得られたデータを有効なものとして用いる第３の手順とを有する。

図面の簡単な説明

図１は、本発明の第１実施形態に係わるデータ処理システムの構成図である。

図２は、図１に示す出力側のデータ処理装置の構成図である。

図３は、図１に示す入力側のデータ処理装置の構成図である。

図４は、図１に示すデータ処理システムの動作例を説明するためのフローチャートである。

図５は、本発明の第２実施形態の通信システムの全体構成図である。

図６は、図５に示す管理装置の機能ブロック図である。

図７は、図６に示す管理装置が行う処理手順の概要を説明するためのフローチャートである。

図８は、図６に示すＡＰ編集ツールおよび管理ツールに係わる処理において用いられるカードを説明するための図である。

図９は、図５に示すＩＣカードの機能ブロック図である。

図１０は、図９に示すメモリに記憶されたデータを説明するための図である。

図１１は、図５に示すＳＡＭモジュールのソフトウェア構成を説明するための図である。

図１２は、図５に示すＳＡＭモジュールのハードウェア構成、並びに外部メモリ７の記憶領域を説明するための図である。

図１３は、図１２に示すＡＰ記憶領域を説明するための図である。

図１４は、アプリケーションエレメントデータを説明するための図である。

図１５は、アプリケーションエレメントデータＡＰＥのタイプを説明するための図である。

図１６は、オーナカードおよびユーザカードの作成手順を説明するためのフローチャートである。

図１７は、相互認証鍵データを説明するための図である。

図１８は、相互認証コードを説明するための図である。

図１９Ａおよび図１９Ｂは、相互認証鍵データとサービスとの関係を説明するための図である。

図２０は、縮退鍵データの生成方法を説明するための図である。

図２１は、縮退鍵データのその他の生成方法を説明するための図である。

図２２は、縮退鍵データの暗号化の階層を説明するための図である。

図２３は、縮退鍵データの特性の一例を説明するための図である。

図２４は、相互認証鍵データの使用形態の一例を説明するための図である。

図２５は、図５に示す管理装置のＳＡＭ管理機能部とＳＡＭユニットとの間の相互認証について説明するためのフローチャートである。

図２６は、図５に示す管理装置のＳＡＭ管理機能部とＳＡＭユニットとの間の相互認証について説明するための図２５の続きのフローチャートである。

図２７は、ＳＡＭユニットの処理を説明するためのフローチャートである。

発明を実施するための最良の形態

これより図面を参照して本発明の好適実施例について説明していく。

第１実施形態

図１は、本実施形態に係わるデータ処理システムの構成図である。

図１に示すように、データ処理システム３０１は、例えば、データ処理装置３０２および３０３を有する。

ここで、データ処理装置３０２が、第１および第２の発明の第１のデータ処理装置、並びに第４の発明のデータ処理装置に対応している。

また、データ処理装置３０３が、第１および第２の発明の第２のデータ処理装置、並びに第７の発明のデータ処理装置に対応している。

図２は、データ処理装置３０２の構成図である。

図２に示すように、データ処理装置３０２は、例えば、メモリ３１０、認証部３１１、暗号化部３１２、インタフェース３１３およびＣＰＵ３１４を有し、これらがバス３０９を介して接続されている。

ここで、メモリ３１０が第４の発明の記憶手段に対応し、認証部３１１が第４の発明の認証手段に対応し、暗号化部３１２が第４の発明の暗号化手段に対応し、

インタフェース３１３が第４の発明の出力手段に対応している。

メモリ３１０は、第１の認証鍵データ３２１、暗号鍵データ３２２およびプログラム３２３を記憶している。

ここで、第１の認証鍵データ３２１が本発明の第１の認証鍵データに対応し、暗号鍵データ３２２が本発明の暗号化データに対応し、プログラム３２３が第５の発明のプログラムに対応している。

認証部３１１は、第１の認証鍵データ３２１を用いて、データ処理装置３０３と相互認証を行う。

暗号化部３１２は、暗号鍵データ３２２を用いて、所定のデータを暗号化する。

インタフェース３１３は、上記暗号化したデータをデータ処理装置３０３に出力する。

ＣＰＵ３１４は、プログラム３２３を実行して、後述するように、データ処理装置３０２の各構成要素を統括的して処理を行う。

図３は、データ処理装置３０３の構成図である。

図３に示すように、データ処理装置３０３は、例えば、メモリ３３０、認証部３３１、復号部３３２、インタフェース３３３およびＣＰＵ３３４を有し、これらがバス３３９を介して接続されている。

ここで、メモリ３３０が第７の発明の記憶手段に対応し、認証部３３１が第７の発明の認証手段に対応し、暗号化部３３２が第７の発明の復号手段に対応し、インタフェース３３３が第７の発明の入力手段に対応している。

メモリ３３０は、第２の認証鍵データ３４１、復号鍵データ３４２およびプログラム３４３を記憶している。

ここで、第２の認証鍵データ３４１が本発明の第２の認証鍵データに対応し、復号鍵データ３４２が本発明の復号データに対応し、プログラム３４３が第７の発明のプログラムに対応している。

認証部３３１は、第２の認証鍵データ３４１を用いて、データ処理装置３０２

と相互認証を行う。

復号部３３２は、復号鍵データ３４２を用いて、インタフェース３３３を介してデータ処理装置３０２から入力したデータを復号する。

インタフェース３３３は、データ処理装置３０２から上記暗号化されたデータを入力する。

ＣＰＵ３３４は、プログラム３４３を実行して、後述するように、データ処理装置３０３の各構成要素を統括的に制御して処理を行う。

以下、図１に示すデータ処理システム３０１の動作例を説明する。

以下に示す処理は、ＣＰＵ３１４によるプログラム３２３の実行、並びにＣＰＵ３３４によるプログラム３４３の実行に応じて行われる。

図４は、当該動作例を説明するためのフローチャートである。

ステップＳＴ９１：

データ処理装置３０２の認証部３１１が第１の認証鍵データ３２１を用い、データ処理装置３０３の認証部３３１が第２の認証鍵データ３４１を用いて、相互認証を行う。

このとき、認証部３１１およびそ３３１は、それぞれ第１の認証鍵データ３２１および３４１を用いて、第１の暗号アルゴリズム並びに当該第１の暗号アルゴリズムに対応する第１の復号アルゴリズムを基に所定のデータの暗号化および復号を行って上記認証を行う。

当該相互認証には、第２実施形態で後述する相互認証の方法が用いられる。

ステップＳＴ９２：

データ処理装置３０２のＣＰＵ３１４が、ステップＳＴ９１の相互認証によりデータ処理装置３０３との間でお互いの正当性が認められたと判断した場合にステップＳＴ９３の処理に進む、そうでない場合には処理を終了する。

ステップＳＴ９３：

データ処理装置３０２の暗号化部３１２が、暗号鍵データ３２２を用いて、第

2の暗号アルゴリズムで所定のデータを暗号化する。

ステップＳＴ９４：

データ処理装置３０２のインタフェース３１３が、ステップＳＴ９３で暗号化したデータをデータ処理装置３０３に出力する。

ステップＳＴ９５：

データ処理装置３０３のＣＰＵ３３４が、ステップＳＴ９１の相互認証によりデータ処理装置３０２との間でお互いの正当性が認められたと判断した場合にステップＳＴ９６の処理に進む、そうでない場合には処理を終了する。

ステップＳＴ９６：

データ処理装置３０３の復号部３３２が、復号鍵データ３４２を用いて、ステップＳＴ９４でインタフェース３３３を介してデータ処理装置３０２から入力した暗号化されたデータを、上記第２の暗号アルゴリズムに対応した第２の復号アルゴリズムで復号する。

ステップＳＴ９７：

データ処理装置３０３のＣＰＵ３３４が、ステップＳＴ９６の復号によって得られた復号データが、適切に復号されたものであるか否かを判断し、適切に復号されたものであると判断した場合にはステップＳＴ９８の処理に進み、そうでない場合には当該復号データを破棄（無効化）する。

ステップＳＴ９８：

データ処理装置３０３のＣＰＵ３３４が、ステップＳＴ９７で得られた復号データを有効なものとして用いて処理を行う。

以上説明したように、データ処理システム３０１によれば、相互認証と暗号化データの生成とを異なる鍵データを用いて行うため、相互認証により用いた第１および第２の認証鍵データが第三者によって不正に取得された場合でも、暗号化データは暗号鍵データを用いて暗号化されているため、当該第三者は当該暗号化データを解読できない。そのため、データ処理システム３０１によれば、暗号化

データを適切に保護できる。

また、データ処理システム３０１によれば、相互認証と暗号化データの生成とで異なる暗号・復号アルゴリズムを用いているため、相互認証で用いた第１の暗号・復号アルゴリズムが第三者に漏れた場合でも、暗号化データは第２の暗号アルゴリズムで暗号化されているため、当該第三者は解読できない。

第２実施形態

図５は、本実施形態の通信システム１の全体構成図である。

図５に示すように、通信システム１は、店舗などに設置されたサーバ装置２、ＩＣカード３、カードリーダ・ライタ４、パーソナルコンピュータ５、ＡＳＰ(Application Service Provider)サーバ装置１９、ＳＡＭ(Secure Application Module) ユニット９ａ，９ｂ,...、管理装置２０、ＩＣモジュール４２が内蔵された携帯通信装置４１を用いて、インターネット１０を介して通信を行ってＩＣカード３あるいは携帯通信装置４１を用いた決済処理などの手続き処理を行う。

通信システム１では、管理装置２０およびＳＡＭユニット９ａ，９ｂが本発明に対応した実施の形態に係わる処理を行う。

すなわち、管理装置２０は、管理者等によって許可された所定の処理をＳＡＭユニット９ａ，９ｂに行わせるために用いるＩＣを内蔵したカード（例えば、後述するオーナカードおよびユーザカード）を発行する処理を行う。これにより、相互認証に用いられる認証鍵データが被認証手段に対して提供される。

また、管理装置２０は、上記発行されたカードを管理者やユーザが用いて、ＳＡＭユニット９ａ，９ｂとの間で上記認証鍵データを基に相互認証を行う。

そして、当該相互認証によって互いの正当性が認められると、暗号化鍵データを用いて暗号化された所定の暗号化データが管理装置２０からＳＡＭユニット９ａ，９ｂに出力され、ＳＡＭユニット９ａ，９ｂが復号鍵データを用いて、当該暗号化データを復号する。

この場合に、管理装置２０が本発明の第１のデータ処理装置および被認証手段

となり、ＳＡＭユニット９ａ，９ｂが本発明の第２のデータ処理装置、認証先および認証手段となる。

図６は、管理装置２０の機能ブロック図である。

図６に示すように、管理装置２０は、例えば、ＡＰ編集ツール５１、管理ツール５２、カードリーダ・ライタ５３、ディスプレイ５４、Ｉ／Ｆ５５および操作部５６を有する。

ＡＰ編集ツール５１および管理ツール５２は、データ処理装置でプログラム(第５の発明のプログラム)を実行して実現してもよいし、電子回路（ハードウェア）によって実現してもよい。

管理ツール５２は、例えば、ＳＡＭ管理機能部５７およびカード管理機能部５８を有する。

カードリーダ・ライタ５３は、以下に示す種々のカードのＩＣとの間で、非接触式あるいは接触式でデータの授受を行う。

ディスプレイ５４は、カード発行画面やＡＰ管理画面を表示するために用いられる。

Ｉ／Ｆ５５は、ＳＡＭユニット９ａ，９ｂとの間で、非接触式あるいは接触式でデータの授受を行う。

操作部５６は、ＡＰ編集ツール５１および管理ツール５２に対して、指示やデータを入力ために用いられる。

図７は、管理装置２０が行う処理手順の概要を説明するためのフローチャートである。

図７において、ステップＳＴ２～ステップＳＴ４が、図４のステップＳＴ９１に対応し、ステップＳＴ５～ＳＴ７が図４のステップＳＴ９３～ＳＴ９８に対応している。

この場合に、管理装置２０がデータ処理装置３０２に対応し、ＳＡＭユニット９ａ，９ｂがデータ処理装置３０３に対応する。

ステップＳＴ１：

管理装置２０は、管理者の操作に応じて、カード管理機能部５８により、カードリーダ・ライタ５３にセットされたデフォルトカード７１を用いて、所定のデータが格納されたオーナカード７２を作成する。また、オーナカード７２を用いてユーザカード７３を作成する。

すなわち、管理装置２０は、ＳＡＭユニット９ａ，９ｂ（本発明の認証手段）に係わる処理のうち、オーナカード７２およびユーザカード７３を用いた被認証手段に許可する処理に関連付けられた相互認証鍵データを用いて、後述するデバイス鍵データを所定の暗号化方法で暗号化して、上記相互認証鍵データを復元困難な縮退鍵データ（本発明の第１の認証鍵データ）を生成する。

そして、管理装置２０は、上記生成した縮退鍵データと、当該縮退鍵データの生成に用いた上記相互認証鍵データを指定する鍵指定データとを、オーナカード７２およびユーザカード７３のＩＣに書き込む。

また、同様に、管理装置２０は、トランスポートカード７４およびＡＰ暗号化カード７５を作成する。

ステップＳＴ２：

オーナカード７２またはユーザカード７３の使用者が、これらのカードを用いて、管理装置２０を介して、当該使用者に権限が与えられた処理をＳＡＭユニット９ａ，９ｂに行わせる場合に、上記使用者が管理装置２０のカードリーダ・ライタ５３に、オーナカード７２またはユーザカード７３のＩＣに記憶された上記鍵指定データを読み込ませる。

管理装置２０のＳＡＭ管理機能部５７は、当該読み込んだ鍵指定データをＳＡＭユニット９ａ，９ｂに出力する。

ステップＳＴ３：

ＳＡＭユニット９ａ，９ｂが、上記鍵指定データが指定する相互認証鍵データを用いて、上記デバイス鍵データを上記所定の暗号化方法で暗号化して縮退鍵デ

ータ（本発明の第２の認証鍵データ）を生成する。

ステップＳＴ４：

ＳＡＭ管理機能部５７がカード７２または７３から読み出した縮退鍵データを用い、ＳＡＭユニット９ａ，９ｂが上記生成した縮退鍵データを用いて、第１の暗号化アルゴリズムおよび第１の復号アルゴリズムを基に相互認証を行う。

ステップＳＴ５：

ステップＳＴ４の相互認証により互いの正当性が認められると、管理装置２０が、暗号鍵データを用いて、第２の暗号化アルゴリズムで所定のデータを暗号化してＳＡＭユニット９ａ，９ｂに出力する。

ステップＳＴ６：

ＳＡＭユニット９ａ，９ｂが、復号鍵データを用いて、ステップＳＴ５で入力した暗号化されたデータを、上記第２の暗号アルゴリズムに対応した第２の復号アルゴリズムで復号する。

ステップＳＴ７：

ＳＡＭユニット９ａ，９ｂが、ステップＳＴ６の復号データが、適切に復号されたものであるか否かを判断し、適切に復号されたものであると判断した場合には、ステップＳＴ６で得られた復号データを有効なものとして用いて、オーナカード７２等に許可した上記鍵データに関連付けられた処理を実行する。

一方、ＳＡＭユニット９ａ，９ｂが、上記復号データが適切に復号されたものではないと判断した場合には、当該復号データを破棄（無効化）する。

図８は、図６に示すＡＰ編集ツール５１および管理ツール５２に係わる処理において用いられるカードを説明するための図である。

図８に示すように、管理装置２０の管理ツール５２を用いて、ＳＡＭユニット９ａ，９ｂにアクセスする場合に、オーナカード７２およびユーザカード７３が用いられる。

また、ＡＰ編集ツール５１で生成したＡＰパッケージファイルを管理ツール５

２に提供する場合に、ＡＰ暗号化カード７５のＩＣに記憶された暗号化鍵データを用いて、当該ＡＰパッケージファイルが暗号化される。

すなわち、図８に示すように、ユーザが、ＡＰ編集ツール５１を用いて、ＳＡＭモジュール８内のアプリケーションプログラムＡＰを構成するアプリケーションエレメントデータＡＰＥを作成する。

そして、ＡＰ編集ツール５１が、単数または複数のアプリケーションエレメントデータＡＰＥを含むＡＰパッケージファイルを作成し、これをＡＰ暗号化カード７５に格納された暗号鍵データを用いて暗号化して管理ツール５２に提供する。

管理ツール５２は、上述したように、ＳＡＭユニット９ａ，９ｂと相互認証を行い、当該相互認証に用いた相互認証鍵データに関連付けて許可されたＳＡＭユニット９ａ，９ｂ内のＡＰ記憶領域に対して、ＡＰ編集ツール５１から受けたＡＰパッケージファイルを書き込む。

また、トランスポートカード７４は、ＳＡＭユニット９ａ，９ｂが保持する鍵データなどのセキュリティに係わるデータを取り出して他の機器に転送したり、保存等するために用いられる。

〔ＩＣカード３および携帯通信装置４１〕

図９は、ＩＣカード３の機能ブロック図である。

図９に示すように、ＩＣカード３は、メモリ５０およびＣＰＵ５１を備えたＩＣ(Integrated Circuit)モジュール３ａを有する。

メモリ５０は、図１０に示すように、クレジットカード会社などのサービス事業者１５＿１が使用する記憶領域５５＿１、サービス事業者１５＿２が使用する記憶領域５５＿２、並びにサービス事業者１５＿３が使用する記憶領域５５＿３を有する。

また、メモリ５０は、記憶領域５５＿１へのアクセス権限を判断するために用いられる鍵データ、記憶領域５５＿２へのアクセス権限を判断するために用いられる鍵データ、並びに記憶領域５５＿３へのアクセス権限を判断するために用い

られる鍵データを記憶している。当該鍵データは、相互認証や、データの暗号化および復号などに用いられる。

また、メモリ５０は、ＩＣカード３あるいはＩＣカード３のユーザの識別データを記憶している。

携帯通信装置４１は、携帯電話網およびインターネット１０を介してＡＳＰサーバ装置１９ａ，１９ｂと通信を行う通信処理部４３と、通信処理部４３との間でデータ授受可能なＩＣモジュール４２とを有し、アンテナからインターネット１０を介してＳＡＭユニット９ａと通信を行う。

ＩＣモジュール４２は、携帯通信装置４１の通信処理部４３とデータ授受を行う点を除いて、前述したＩＣカード３のＩＣモジュール３ａと同じ機能を有している。

なお、携帯通信装置４１を用いた処理は、ＩＣカード３を用いた処理と同様に行われ、ＩＣモジュール４２を用いた処理はＩＣモジュール３ａを用いた処理と同様に行われるため、以下の説明では、ＩＣカード３およびＩＣモジュール３ａを用いた処理について例示する。

以下、ＳＡＭユニット９ａ，９ｂについて説明する。

図５に示すように、ＳＡＭユニット９ａ，９ｂは、外部メモリ７とＳＡＭモジュール８とを有する。

ここで、ＳＡＭモジュール８は、半導体回路として実現してもよいし、筐体内に複数の回路を収容した装置として実現してもよい。

〔ＳＡＭモジュール８のソフトウェア構成〕

ＳＡＭモジュール８は、図１１に示すようなソフトウェア構成を有している。

図１１に示すように、ＳＡＭモジュール８は、下層から上層に向けて、ハードウェアＨＷ層、周辺ＨＷに対応したＲＴＯＳカーネルなどを含めたドライバ層（ＯＳ層）、論理的にまとまった単位の処理を行う下位ハンドラ層、アプリケーション固有のライブラリなどをまとめた上位ハンドラ層およびＡＰ層を順に有している。

ここで、ＡＰ層では、図５に示すクレジットカード会社などのサービス事業者１５＿１，１５＿２，１５＿３によるＩＣカード３を用いた手続きを規定したアプリケーションプログラムＡＰ＿１，ＡＰ＿２，ＡＰ＿３が、外部メモリ７から読み出されて動作している。

ＡＰ層では、アプリケーションプログラムＡＰ＿１，ＡＰ＿２，ＡＰ＿３相互間、並びに上位ハンドラ層との間にファイアウォールＦＷが設けられている。

〔ＳＡＭモジュール８のハードウェア構成〕

図１２は、ＳＡＭモジュール８のハードウェア構成、並びに外部メモリ７の記憶領域を説明するための図である。

図１２に示すように、ＳＡＭモジュール８は、例えば、メモリＩ／Ｆ６１、外部Ｉ／Ｆ６２、メモリ６３、認証部６４およびＣＰＵ６５を有し、これらがバス６０を介して接続されている。

また、ＳＡＭモジュール８が、第７の発明のデータ処理装置に対応し、以下に示す各手順を含むプログラムを実行して、その機能を実現してもよい。

メモリＩ／Ｆ６１は、外部メモリ７との間でデータ授受を行う。

外部Ｉ／Ｆ６２は、図５に示すＡＳＰサーバ装置１９ａ，１９ｂおよび管理装置２０との間で、データおよびコマンドの授受を行う。

メモリ６３は、後述するＳＡＭユニット９ａ，９ｂの相互認証などに用いられる種々の鍵データなどを記憶する。当該鍵データは、外部メモリ７のＡＰ管理用記憶領域２２１に記憶されていてもよい。

認証部６４は、後述する相互認証に係わる処理を行う。認証部６４は、例えば、所定の鍵データを用いた暗号化および復号などを処理を行う。

ＣＰＵ６５は、ＳＡＭモジュール８の処理を統括して制御する。

ＣＰＵ６５は、後述するように、相互認証で正当な相手であることを確認すると、被認証手段に対して、後述する相互認証鍵データに関連付けられた処理を許可し、これを実行する。

ＳＡＭモジュール８による相互認証処理については、後に詳細に説明する。

〔外部メモリ７〕

図１２に示すように、外部メモリ７の記憶領域には、サービス事業者１５＿１のアプリケーションプログラムＡＰ＿１が記憶されるＡＰ記憶領域２２０＿１（サービスＡＰリソース領域)、サービス事業者１５＿２のアプリケーションプログラムＡＰ＿２が記憶されるＡＰ記憶領域２２０＿２、サービス事業者１５＿３のアプリケーションプログラムＡＰ＿３が記憶されるＡＰ記憶領域２２０＿３、並びにＳＡＭモジュール２０８の管理者が使用するＡＰ管理用記憶領域２２１（システムＡＰリソース領域および製造者ＡＰリソース領域）がある。

ＡＰ記憶領域２２０＿１に記憶されているアプリケーションプログラムＡＰ＿１は、図１３に示すように、後述する複数のアプリケーションエレメントデータＡＰＥによって構成されている。ＡＰ記憶領域２２０＿１へのアクセスは、ファイアウォールＦＷ＿１（図１２に図示）によって制限されている。

ＡＰ記憶領域２２０＿２に記憶されているアプリケーションプログラムＡＰ＿２は、図１３に示すように、複数のアプリケーションエレメントデータＡＰＥによって構成されている。ＡＰ記憶領域２２０＿２へのアクセスは、ファイアウォールＦＷ＿２（図１２に図示）によって制限されている。

ＡＰ記憶領域２２０＿３に記憶されているアプリケーションプログラムＡＰ＿３は、図１３に示すように、複数のアプリケーションエレメントデータＡＰＥによって構成されている。ＡＰ記憶領域２２０＿３へのアクセスは、ファイアウォールＦＷ＿３（図１２に図示）によって制限されている。

本実施形態では、上記アプリケーションエレメントデータＡＰＥは、例えば、ＳＡＭユニット９ａの外部から外部メモリ７にダウンロードされる最小単位である。各アプリケーションプログラムを構成するアプリケーションエレメントデータＡＰＥの数は、対応するサービス事業者が任意に決定できる。

また、アプリケーションプログラムＡＰ＿１，ＡＰ＿２，ＡＰ＿３は、例えば、

それぞれ図５に示すパーソナルコンピュータ１５＿１，１５＿２，１５＿３を用いて、サービス事業者１６＿１，１６＿２，１６＿３によって作成され、ＳＡＭモジュール８を介して外部メモリ７にダウンロードされる。

なお、ＡＰ管理用記憶領域２２１に記憶されたプログラム、並びにデータも、上述したアプリケーションエレメントデータＡＰＥを用いて構成されている。

図１４は、上述したアプリケーションエレメントデータＡＰＥを説明するための図である。

アプリケーションエレメントデータＡＰＥは、図１４に示すように、ＡＰＥの属性（種別）を基に規定された分類を示すＡＰＥタイプによって規定されたインスタンスを用いて構成される。

各インスタンスは、エレメントＩＤと、エレメントプロパティと、エレメントバージョンとによって規定されている。

ＡＰＥタイプを基に、当該アプリケーションエレメントデータＡＰＥが、図１２に示すサービスＡＰ記憶領域２２０＿１，２２０＿２，２２０＿３およびＡＰ管理用記憶領域２２１の何れに格納されるかが規定される。

サービスＡＰ記憶領域２２０＿１は、各サービス事業者がアクセス可能なデータを記憶する。

なお、ＡＰ管理用記憶領域２２１は、システムの管理者がアクセス可能なデータを記憶するシステムＡＰ記憶領域（図示せず）と、システムの製造者がアクセス可能なデータを記憶する製造者ＡＰ記憶領域（図示せず）とを有する。

また、サービスＡＰ記憶領域２２０＿１，２２０＿２，２２０＿３およびＡＰ管理用記憶領域２２１によって、ＡＰ記憶領域が構成される。

本実施形態では、上述したサービスＡＰ記憶領域２２０＿１，２２０＿２，２２０＿３およびＡＰ管理用記憶領域２２１の各々にはＩＤ（ＡＰ記憶領域ＩＤ）が割り当てられており、ＡＰＥタイプ、インスタンス、並びにエレメントバージョンの各々には識別用の番号（ＡＰＥタイプ番号、インスタンス番号、並びにエ

レメントバージョン番号）が割り当てられている。

図１５は、ＡＰＥタイプの一例を説明するための図である。

図１５に示すように、ＡＰＥタイプには、ＩＣシステム鍵データ、ＩＣエリア鍵データ、ＩＣサービス鍵データ、ＩＣ縮退鍵データ、ＩＣ鍵変更パッケージ、ＩＣ発行鍵パッケージ、ＩＣ拡張発行鍵パッケージ、ＩＣエリア登録鍵パッケージ、ＩＣエリア削除鍵パッケージ、ＩＣサービス登録鍵パッケージ、ＩＣサービス削除鍵パッケージ、ＩＣメモリ分割鍵パッケージ、ＩＣメモリ分割素鍵パッケージ、障害記録ファイル、相互認証用鍵、パッケージ鍵、ネガリストおよびサービスデータテンポラリファイルがある。

各ＡＰＥタイプには、ＡＰＥタイプ番号が割り当てられている。

以下、図１５に示すＡＰＥタイプのうち一部を説明する。

ＩＣシステム鍵データ、ＩＣエリア鍵データ、ＩＣサービス鍵データおよびＩＣ縮退鍵データは、ＩＣカード３およびＩＣモジュール４２のメモリ５０に対してのデータの読み書き操作に用いられるカードアクセス鍵データである。

相互認証用鍵データ同一ＳＡＭ内にあるＡＰ間相互認証にも使用される。ＳＡＭ相互認証用鍵データとは、対応するアプリケーションエレメントデータＡＰＥを同一ＳＡＭ内の他のＡＰまたは他のＳＡＭからアクセスする際に用いられる鍵データである。

ＩＣメモリ分割用鍵パッケージは、サービス事業者がＩＣカード３を用いたサービスの運用開始前に、外部メモリ７やＩＣカード３のメモリの記憶領域を分割するために使用するデータである。

ＩＣエリア登録鍵パッケージは、サービス事業者がＩＣカード３を用いたサービスの運用開始前に、ＩＣカード３のメモリの記憶領域にエリア登録を行う場合に使用するデータである。

ＩＣエリア削除用鍵パッケージは、カードアクセス鍵データからＳＡＭ内部で自動生成が可能なパッケージである。

ＩＣサービス登録用鍵パッケージは、サービス事業者がＩＣカード３を用いたサービスの運用開始前に、外部メモリ７のアプリケーションエレメントデータＡＰＥを登録するために用いられる。

ＩＣサービス削除用鍵パッケージは、外部メモリ７に登録されているアプリケーションエレメントデータＡＰＥを削除するために用いられる。

〔オーナカード７２およびユーザカード７３の作成〕

図１６は、オーナカード７２およびユーザカード７３の作成手順を説明するためのフローチャートである。

図１６は、図７に示すステップＳＴ１を詳細に示すものである。

ステップＳＴ１１：

例えば、管理者が、オーナカード７２を作成する場合には、オーナカード７２の使用者に許可するＳＡＭユニット９ａ，９ｂに係わる処理を選択する。

また、管理者等が、ユーザカード７３を作成する場合に、ユーザカード７３の使用者に許可するＳＡＭユニット９ａ，９ｂに係わる処理を選択する。

ＳＡＭユニット９ａ，９ｂに係わる処理には、例えば、ＳＡＭユニット９ａ，９ｂが提供する機能を実行する処理、またはＳＡＭユニット９ａ，９ｂが保持するデータ（例えば、アプリケーションエレメントデータＡＰＥ）へのアクセスなどがある。

ステップＳＴ１２：

管理者等が、ステップＳＴ１１で選択した処理に関連付けられた相互認証鍵データを選択して、管理装置２０のカード管理機能部５８に入力あるいは指定する。

当該相互認証鍵データについては後に詳細に説明する。

ステップＳＴ１３：

管理装置２０のカード管理機能部５８が、ステップＳＴ１２で選択された単数または複数の相互認証鍵データを用いて後述する縮退処理方法を基に縮退鍵データを生成する。

当該縮退処理については後に詳細に説明する。

ステップＳＴ１４：

管理装置２０のカード管理機能部５８が、ステップＳＴ１３で縮退鍵データの生成に用いた、相互認証鍵データを識別する相互認証コードを示す鍵指定データを生成する。

当該鍵指定データは、オーナカード７２またはユーザカード７３の使用者が取得した、ＳＡＭユニット９ａ，９ｂに係わる処理の実行権限を示すデータとなる。

ステップＳＴ１５：

管理装置２０のカード管理機能部５８が、ステップＳＴ１３で生成した縮退鍵データと、ステップＳＴ１４で生成した鍵指定データとを、オーナカード７２またはユーザカード７３のＩＣに書き込む。

ステップＳＴ１６：

管理装置２０のカード管理機能部５８が、ステップＳＴ１３の縮退鍵データの生成に用いた、相互認証鍵データをＳＡＭユニット９ａ，９ｂに登録する。

以下、上述した図１６に示すステップＳＴ１２で選択する対象となる相互認証鍵データについて説明する。

図１７は、図１６に示すステップＳＴ１２で選択する対象となる相互認証鍵データを説明するための図である。

図１７に示すように、当該相互認証鍵データには、例えば、デバイス鍵データ、ターミネーション鍵データ、製造設定サービス相互認証鍵データ、機器管理サービス相互認証鍵データ、通信管理サービス相互認証鍵データ、相互認証サービス相互認証鍵データ、ＡＰ記憶領域管理サービス相互認証鍵データ、サービスＡＰ記憶領域相互認証鍵データ、システムＡＰ記憶領域相互認証鍵データ、並びに製造者ＡＰ記憶領域相互認証鍵データがある。

また、図１７および図１８に示すように、相互認証鍵データの相互認証コードが、図１４を用いて説明したＡＰ記憶領域ＩＤ、エレメントタイプ番号、エレメ

ントインスタンス番号およびエレメントバージョン番号から構成される。

以下、上述した図１６に示すステップＳＴ１４で生成する鍵指定データについて説明する。

当該鍵指定データは、上述した複数の相互認証鍵データの相互認証コードを用いて構成される、相互認証コードリストである。

図１９Ａおよび図１９Ｂは、鍵指定データの一例を説明するための図である。

図１６のステップＳＴ１２で、例えば、図１７に示すデバイス鍵データ、機器管理サービス相互認証鍵データ、通信管理サービス相互認証鍵データ、ＡＰ記憶領域管理サービス相互認証鍵データ、サービスＡＰ記憶領域相互認証鍵データ、並びにターミネーション鍵データが選択された場合には、図１９Ａに示すように、当該選択された全ての相互認証鍵データの相互認証コードを示す鍵指定データが生成される。

図１６に示すステップＳＴ１３において、図１９Ａに示す相互認証コードの相互認証鍵データを用いて縮退鍵データが生成された場合には、当該縮退鍵データを用いたＳＡＭユニット９ａ，９ｂとの相互認証により、管理装置２０に対して、図１９Ｂに示すように、機器管理サービス、通信管理サービス、ＩＣサービス（ＩＣカード３およびＩＣモジュール４２１に関するサービス）、相互認証サービスおよびＡＰ記憶領域管理サービスが許可される。

このように、本実施形態では、ＳＡＭユニット９ａ，９ｂの機能と、ＳＡＭユニット９ａ，９ｂが保持するデータ（例えば、アプリケーションエレメントデータＡＰＥ）へのアクセスを含む複数の処理にそれぞれ関連付けられた相互認証鍵データを用いて縮退鍵データを生成できる。

これにより、単数の縮退鍵データを用いた相互認証により、ＳＡＭユニット９ａ，９ｂが、ＳＡＭユニット９ａ，９ｂの機能と、ＳＡＭユニット９ａ，９ｂが保持するデータへのアクセスとの双方について、それらを被認証手段に対して許可するか否かを一括して判断できる。

そして、ＳＡＭユニット９ａ，９ｂは、被認証手段が正当であると認証した場合に、当該被認証手段の指示に応じて、上記相互認証鍵データに関連付けられた所定の機能に係わる処理を実行すると共に、ＳＡＭユニット９ａ，９ｂが保持するデータへの上記被認証手段からのアクセスを許可する。

以下、図１６に示すステップＳＴ１３の縮退処理方法について説明する。

図２０は、当該縮退処理方法を説明するためのフローチャートである。

ステップＳＴ２１：

管理装置２０のカード管理機能部５８が、デバイス鍵データをメッセージとし、図１６に示すステップＳＴ１２で選択されたデバイス鍵データおよびターミネーション鍵データ以外の相互認証鍵データのうち最初の一つを暗号鍵として用いて、デバイス鍵データを暗号化し、中間鍵データを生成する。

ここで、ステップＳＴ１２で選択されたデバイス鍵データおよびターミネーション鍵データ以外の相互認証鍵データが一つの場合には、カード管理機能部５８は、上記中間鍵データを用いて次のステップＳＴ２２の処理を行う。

一方、ステップＳＴ１２で選択されたデバイス鍵データおよびターミネーション鍵データ以外の相互認証鍵データが２以上の場合には、カード管理機能部５８は、上記中間鍵データをメッセージとして、次の相互認証鍵データを暗号鍵として用いて暗号化を行う。

カード管理機能部５８は、ステップＳＴ１２で選択されたデバイス鍵データおよびターミネーション鍵データ以外の全ての相互認証鍵データを暗号鍵として用いて上記暗号化を行うまで上記処理を繰り返し、終了したらステップＳＴ２２の処理に進む。

ステップＳＴ２２：

カード管理機能部５８が、ステップＳＴ２１で得られた中間鍵データをメッセージとして、ターミネーション鍵データを暗号鍵として用いて暗号化を行って縮退鍵データを生成する。

当該ターミネーショ鍵データは、改竄防止鍵データであり、管理者のみが保持している。

これにより、管理者以外の者が、不正に縮退鍵データを改竄することを防止できる。

以下、上述したターミネーション鍵データとして、管理者（オーナ）のみが所有するオーナターミネーション鍵データと、上記管理者から権限を与えられたユーザが所有するユーザターミネーション鍵データとを用いて、所定の縮退処理方法で、縮退鍵データを生成する場合を説明する。

図２１は、当該縮退処理方法を説明するためのフローチャートである。

図２１において、ステップＳＴ３１，Ｓ３２の処理は、ターミネーション鍵データとして、上記オーナターミネーション鍵データを用いる点を除いて、図２０を用いて説明したステップＳＴ２１，２２の処理と同じである。

ステップＳＴ３２で生成された縮退鍵データは、ユーザターミネーション鍵データを与えられたユーザが、拡張できるという意味で拡張可能な縮退鍵データである。

ステップＳＴ３３：

管理装置２０のカード管理機能部５８が、オーナが生成した拡張可能縮退鍵データをメッセージとし、ユーザが選択したユーザターミネーション鍵データ以外の相互認証鍵データのうち最初の一つを暗号鍵として用いて、デバイス鍵データを暗号化し、中間鍵データを生成する。

ここで、上記選択されたユーザターミネーション鍵データ以外の相互認証鍵データが一つの場合には、カード管理機能部５８は、上記中間鍵データを用いて次のステップＳＴ２２の処理を行う。

一方、上記選択されたユーザターミネーション鍵データ以外の相互認証鍵データが２以上の場合には、カード管理機能部５８は、上記中間鍵データをメッセージとして、次の相互認証鍵データを暗号鍵として用いて暗号化を行う。

カード管理機能部５８は、上記選択されたユーザターミネーション鍵データ以外の全ての相互認証鍵データを暗号鍵として用いて上記暗号化を行うまで上記処理を繰り返し、終了したらステップＳＴ３４の処理に進む。

ステップＳＴ３４：

カード管理機能部５８が、ステップＳＴ３３で得られた中間鍵データをメッセージとして、ユーザターミネーション鍵データを暗号鍵として用いて暗号化を行って縮退鍵データを生成する。

当該ユーザターミネーショ鍵データは、改竄防止鍵データであり、上記オーナおよび上記ユーザのみが保持している。

これにより、上記オーナおよび上記ユーザ以外の者が、不正に縮退鍵データを改竄することを防止できる。

図２１に示す処理によって生成された縮退鍵データは、図２２に示すような階層で相互認証鍵が暗号化されたものになる。

また、本実施形態では、単数の相互認証鍵データ（例えば、図１７に示すサービス、システム、製造者ＡＰ記憶領域相互認証鍵データ）に、複数のアプリケーションエレメントデータＡＰＥを関連付けてもよい。

これにより、縮退鍵データを用いた認証により、ＳＡＭユニット９ａ，９ｂが、単数の相互認証鍵データに関連付けられたアプリケーションエレメントデータＡＰＥへのアクセスを許可するか否かを一括して判断できる。

例えば、図２３では、相互認証鍵データ５００に，アプリケーションエレメントデータＡＰＥのインスタンスａのパーミッションＣと、インスタンスｂのパーミッションＢとが関連付けられている。そのため、相互認証鍵データ５００を縮退した縮退鍵データを用いた認証が成功すれば、ＳＡＭユニット９ａ，９ｂがインスタンスａ，ｂの双方へのアクセスを許可する。

本実施形態では、図１７を用いて説明した相互認証鍵データの全てある一部について、図２４に示すように、オンライン相互認証鍵データＭＫ１とオフライン

相互認証鍵データＭＫ２とをペアで用いる。

この場合には、相互認証を行う場合にはオンライン鍵データＭＫ１を用い、相互認証を行った相手とはデータ授受を行う場合には、それに対応するオフライン鍵データＭＫ２を用いて授受するデータを暗号化する。

これにより、仮にオンライン鍵データＭＫ１が不正に他人に取得された場合でも、被認証手段と認証手段とで授受するデータはオフライン鍵データＭＫ２で暗号化されているため、その情報が不正に漏れることを防止できる。

すなわち、第１実施形態における第１の認証鍵データ３２１がオンライン鍵データＭＫ１に対応し、第１実施形態における暗号鍵データ３２２がオフライン鍵データＭＫ２に対応している。また、第１実施形態における第２の認証鍵データ３４１がオンライン鍵データＭＫ１に対応し、第１実施形態における復号鍵データ３４２がオフライン鍵データＭＫ２に対応している。

以下、例えば、図７に示すステップＳＴ３などで行われる管理装置２０のＳＡＭ管理機能部５７とＳＡＭユニット９ａ，９ｂとの間の相互認証について説明する。

この場合に、管理装置２０が被認証手段となり、ＳＡＭユニット９ａ，９ｂが認証手段となる。

図２５および図２６は、管理装置２０のＳＡＭ管理機能部５７とＳＡＭユニット９ａとの間の相互認証について説明するためのフローチャートである。

ＳＡＭユニット９ｂについても、以下に示すＳＡＭユニット９ａの場合と同じである。

ステップＳＴ５１：

先ず、管理者またはユーザが、オーナカード７２またはユーザカード７３を、カードリーダ・ライタ５３にセットする。

そして、オーナカード７２およびユーザカード７３に記憶された縮退鍵データＫａ（本発明の第１の認証鍵データ）および鍵指定データが、管理装置２０のＳ

ＡＭ管理機能部５７に読み込まれる。

ＳＡＭ管理機能部５７が、乱数Ｒａを発生する。

ステップＳＴ５２：

ＳＡＭ管理機能部５７が、ステップＳＴ５１で読み込んだ縮退鍵データＫａを用いて、ステップＳＴ５１で生成した乱数Ｒａを、暗号化アルゴリズム１で暗号化してデータＲａ’を生成する。

ステップＳＴ５３：

ＳＡＭ管理機能部５７が、ステップＳＴ５１で読み込んだ鍵指定データと、ステップＳＴ５２で生成したデータＲａ’とをＳＡＭユニット９ａに出力する。

ＳＡＭユニット９ａは、図１２に示す外部Ｉ／Ｆ６２を介して、当該鍵指定データおよびデータＲａ’を入力して、これをメモリ６３に格納する。

ステップＳＴ５４：

ＳＡＭユニット９ａの認証部６４が、メモリ６３あるいは外部メモリ７に記憶された相互認証鍵データのなかから、ステップＳＴ５３で入力した鍵指定データが示す相互認証鍵データを特定する。

ステップＳＴ５５：

ＳＡＭユニット９ａの認証部６４が、ステップＳＴ５４で特定した相互認証鍵データを用いて、図２０あるいは図２１を用いて前述した縮退処理を行って縮退鍵データＫｂを生成する。

ステップＳＴ５６：

ＳＡＭユニット９ａの認証部６４が、ステップＳＴ５５で生成した縮退鍵データＫｂを用いて、上記暗号化アルゴリズム１に対応した復号アルゴリズム１で、ステップＳＴ５３で入力したデータＲａ’を復号して乱数Ｒａを生成する。

ステップＳＴ５７：

ＳＡＭユニット９ａの認証部６４が、上記縮退鍵データＫｂを用いて、暗号化アルゴリズム２で、ステップＳＴ５６で生成した乱数Ｒａを暗号化して、データ

Ｒａ’’を生成する。

ステップＳＴ５８：

ＳＡＭユニット９ａの認証部６４が、乱数Ｒｂを生成する。

ステップＳＴ５９：

ＳＡＭユニット９ａの認証部６４が、上記縮退鍵データＫｂを用いて、ステップＳＴ５８で生成した乱数Ｒｂを、暗号化アルゴリズム２で暗号化してデータＲｂ’を生成する。

ステップＳＴ６０：

ＳＡＭユニット９ａの認証部６４が、ステップＳＴ５７で生成したデータＲａ’’と、ステップＳＴ５９で生成したデータＲｂ’とを管理装置２０に出力する。

ステップＳＴ６１：

管理装置２０のＳＡＭ管理機能部５７が、縮退鍵データＫａを用いて、上記暗号アルゴリズム２に対応した復号アルゴリズム２で、ステップＳＴ６０で入力したデータＲａ’’およびＲｂ’を復号してデータＲａ，Ｒｂを生成する。

ステップＳＴ６２：

管理装置２０のＳＡＭ管理機能部５７が、ステップＳＴ５１で生成した乱数Ｒａと、ステップＳＴ６１で生成したデータＲａとを比較する。

そして、ＳＡＭ管理機能部５７が、上記比較と結果が同じであることを示す場合に、ＳＡＭユニット９ａが保持する上記縮退鍵データＫｂが、ＳＡＭ管理機能部５７が保持する上記縮退鍵データＫａと同じであり、ＳＡＭユニット９ａが正当な認証手段であると認証する。

ステップＳＴ６３：

管理装置２０のＳＡＭ管理機能部５７が、縮退鍵データＫａを用いて、暗号化アルゴリズム１で、ステップＳＴ６１で生成したデータＲｂを暗号化して、データＲｂ’’を生成する。

ステップＳＴ６４：

管理装置２０のＳＡＭ管理機能部５７が、ステップＳＴ６３で生成したデータＲｂ’’をＳＡＭユニット９ａに出力する。

ステップＳＴ６５：

ＳＡＭユニット９ａの認証部６４が、縮退鍵データＫｂを用いて、ステップＳＴ６４で入力したデータＲｂ’’を、復号アルゴリズム１で復号してデータＲｂを生成する。

ステップＳＴ６６：

ＳＡＭユニット９ａの認証部６４が、ステップＳＴ５８で生成した乱数Ｒｂと、ステップＳＴ６５で生成したデータＲｂとを比較する。

そして、認証部６４が、上記比較と結果が同じであることを示す場合に、ＳＡＭユニット９ａが保持する上記縮退鍵データＫｂが、ＳＡＭ管理機能部５７が保持する上記縮退鍵データＫａと同じであり、ＳＡＭ管理機能部５７が正当な被認証手段であると認証する。

上述した図２５および図２５を用いて説明した相互認証方法は、例えば、図４に示すステップＳＴ９１の相互認証で用いてもよい。

この場合には、データ処理装置３０２が上述した管理装置２０に対応した処理を行い、データ処理装置３０３が上述したＳＡＭユニット９ａ，９ｂに対応した処理を行う。

以下、図２５および図２６を用いて説明した相互認証の結果を基に、ＳＡＭユニット９ａ，９ｂが行う処理を説明する。

図２７は、ＳＡＭユニット９ａ，９ｂの処理を説明するための図である。

ステップＳＴ７１：

図１２に示すＳＡＭユニット９ａ，９ｂのＣＰＵ６５が、図２６に示すステップＳＴ６６において、認証部６４が認証手段が正当であると認証したか否かを判断し、正当であると認証したと判断した場合にはステップＳＴ７２の処理に進み、そうでない場合には処理を終了する（すなわち、処理に係わる権限を有しないと

判断し、処理を実行しない)。

ステップＳＴ７２：

ＳＡＭユニット９ａ，９ｂのＣＰＵ６５が、復号鍵データを用いて、管理装置２０から入力した暗号化されたデータ（暗号化データ）を、上記第２の暗号アルゴリズムに対応した第２の復号アルゴリズムで復号する。

そして、ＳＡＭユニット９ａ，９ｂが、上記復号データが、適切に復号されたものであるか否かを判断し、適切に復号されたものであると判断した場合には、当該復号データを有効なものとして用いて、オーナカード７２等に許可した上記相互認証鍵データに関連付けられた処理を実行する。

一方、ＳＡＭユニット９ａ，９ｂが、上記復号データが適切に復号されたものではないと判断した場合には、当該復号データを破棄（無効化）する。

以上説明したように、通信システム１によれば、管理装置２０とＳＡＭユニット９ａ，９ｂとの間の相互認証と、管理装置２０からＳＡＭユニット９ａに出力する暗号化データの生成とを異なる鍵データを用いて行うため、相互認証により用いた縮退鍵データが第三者によって不正に取得された場合でも、暗号化データは暗号鍵データを用いて暗号化されているため、当該第三者は当該暗号化データを解読できない。そのため、暗号化データを適切に保護できる。

また、通信システム１によれば、相互認証と暗号化データの生成とで異なる暗号・復号アルゴリズムを用いることで、相互認証で用いた暗号・復号アルゴリズムが第三者に漏れた場合でも、暗号化データは他の暗号アルゴリズムで暗号化されているため、当該第三者は解読できない。

また、管理装置２０によれば、図１６および図２０等を用いて説明したように、ＳＡＭユニット９ａ，９ｂに係わる処理に関連付けられた複数の相互認証鍵データを用いて縮退処理を行い、縮退鍵データを生成する。

そして、オーナカード７２やユーザカード７３に、当該縮退鍵データ、並びにその生成に用いた相互認証鍵データを特定するための鍵指定データを書き込む。

また、オーナカード７２等を用いた管理装置２０とＳＡＭユニット９ａ，９ｂとの間で、図２５～図２７を用いた相互認証を行うことで、ＳＡＭユニット９ａが管理装置２０から受けた鍵指定データを基に縮退鍵データを生成し、当該縮退鍵データが管理装置２０が保持するものと一致した場合に、被認証手段である管理装置２０の正当性を確認できる。

また、その確認と共に、鍵指定データによって指定された相互認証鍵データに関連付けられた処理を、管理装置２０に許可された処理であると判断できる。

そのため、認証手段であるＳＡＭユニット９ａ，９ｂは、従来のように全ての被認証手段（例えば、オーナカード７２およびユーザカード７３を用いた管理装置２０等）に対応した相互認証鍵データを保持する必要がなく、しかも、被認証手段に許可した処理を管理テーブルで管理する必要もなく、処理負担が軽減される。

本発明は上述した実施形態には限定されない。

本発明は、例えば、オーナカード７２、ユーザカード７３、トランスポートカード７４およびＡＰ暗号化カード７５の何れかのカードのＩＣに、そのカードの使用者の生体情報を記憶させ、ＳＡＭユニット９ａ，９ｂが、上述した相互認証と共に、当該カードに記憶された生体情報をさらに用いて、その使用者の正当性を認証してもよい。

例えば、上述した実施形態では、ＳＡＭユニット９ａ，９ｂが管理装置２０と相互認証を行う場合を例示したが、ＳＡＭユニット９ａ，９ｂがＡＳＰサーバ装置１９ａ，１９ｂや他のＳＡＭユニットなどの被認証手段と認証を行ってもよい。この場合には、当該被認証手段が、上述した縮退鍵データおよび鍵指定データを保持する。

また、上述した実施形態では、オーナカード７２およびユーザカード７３が、上述した縮退鍵データおよび鍵指定データを保持する場合を例示したが、その他の携帯装置などに、これらのデータを保持させてもよい。

産業上の利用可能性

本発明は、認証結果を基に所定の処理を行うデータ処理システムに適用可能である。

請 求 の 範 囲

1． 第1のデータ処理装置が第1の認証鍵データおよび暗号鍵データを保持し、第2のデータ処理装置が前記第1の認証鍵データに対応した第2の認証鍵データと前記暗号鍵データに対応した復号鍵データとを保持する場合に、前記第1のデータ処理装置と前記第2のデータ処理装置とが行うデータ処理方法であって、

前記第1のデータ処理装置が前記第1の認証鍵データを用い、前記第2のデータ処理装置が前記第2の認証鍵データを用いて、前記第1のデータ処理装置と前記第2のデータ処理装置との間で認証を行う第1の工程と、

前記第2のデータ処理装置が、前記第1の工程の前記認証により前記第1のデータ処理装置の正当性を認めた場合に、前記第1のデータ処理装置が前記暗号鍵データを用いて暗号化を行って前記第2のデータ処理装置に提供した暗号化データを、前記復号鍵データを用いて復号する第2の工程と、

前記第2のデータ処理装置が、前記第2の工程の前記復号によって得た復号データが適切に復号されたものであると判断した場合に、前記復号データを有効なものとして用いる第3の工程と

を有するデータ処理方法。

2． 前記第1の工程において、前記第1のデータ処理装置および前記第2のデータ処理装置が、第1の暗号化アルゴリズム並びに前記第1の暗号化アルゴリズムに対応した第1の復号アルゴリズムを基に、所定のデータの暗号化および復号を行って前記認証を行い、

前記第2の工程において、前記第2のデータ処理装置が、第2の暗号化アルゴリムを基に暗号化された前記暗号化データを、前記第2の暗号化アルゴリズムに対応した第2の復号アルゴリズムを基に前記復号する

請求項1に記載のデータ処理方法。

3． 前記第2の工程において、前記第2のデータ処理装置が、前記第1のエ

程の前記認証により、前記第１の認証鍵データと前記第２の認証鍵データとが同じであると判断した場合に、前記第１のデータ処理装置の正当性を認める

請求項１に記載のデータ処理方法。

４．　前記第１の認証鍵データが所定の鍵データを用いて所定の生成方法で生成されている場合に、

前記第１の工程は、

前記第１のデータ処理装置が、前記第１の認証鍵データの生成に用いられた鍵データを指定する鍵指定データを前記第２のデータ処理装置に提供する第４の工程と、

前記第２のデータ処理装置が、前記第４の工程で受けた前記鍵指定データが指定する前記鍵データを用いて前記所定の生成手法で前記第２の認証鍵データを生成する第５の工程と、

前記第１のデータ処理装置が前記第１の認証鍵データを用い、前記第２のデータ処理装置が前記第５の工程で生成した前記第２の認証鍵データを用いて、前記認証を行う第６の工程と、

前記第２のデータ処理装置が、前記第６の工程の前記認証により、前記第１の認証鍵データと前記第２の認証鍵データとが同じであると判断すると、前記第１のデータ処理装置の正当性を認める第７の工程と

を有する請求項１に記載のデータ処理方法。

５．　第１の認証鍵データおよび暗号鍵データを保持する第１のデータ処理装置と、

前記第１の認証鍵データに対応した第２の認証鍵データと前記暗号鍵データに対応した復号鍵データとを保持する第２のデータ処理装置と

を有し、

前記第１のデータ処理装置が、前記第１の認証鍵データを用い、前記第２のデータ処理装置が前記第２の認証鍵データを用いて、前記第１のデータ処理

装置と前記第２のデータ処理装置との間で認証を行い、

前記第２のデータ処理装置が、前記認証により前記第１のデータ処理装置の正当性を認めた場合に、前記第１のデータ処理装置が前記暗号鍵データを用いて暗号化を行って前記第２のデータ処理装置に提供した暗号化データを、前記復号鍵データを用いて復号し、

前記第２のデータ処理装置が、前記復号によって得た復号データが適切に復号されたものであると判断した場合に、前記復号データを有効なものとして用いる　データ処理システム。

６．　認証鍵データおよび暗号鍵データを保持するデータ処理装置が行うデータ処理方法であって、

前記認証鍵データを用いて、認証先と認証を行う第１の工程と、

前記第１の工程の前記認証の後に、前記暗号鍵データを用いて所定のデータを暗号化する第２の工程と、

前記第２の工程の前記暗号化により得られたデータを前記認証先に出力する第３の工程と

を有するデータ処理方法。

７．　鍵データを保持する前記認証先の認証手段が、第１の認証鍵データを保持する前記データ処理装置から指定された前記鍵データを用いて所定の生成手法を基に第２の認証鍵データを生成し、前記第２の認証鍵データを用いて前記データ処理装置と認証を行い、当該認証により、前記第１の認証鍵データと前記第２の認証鍵データとが同じであることを確認したことを条件に、前記第３の工程で出力された前記データを有効なものとして用いる場合に、

前記第１の工程は、

前記所定の生成方法を基に前記第１の認証鍵データを生成したときに用いた前記鍵データを指定する鍵指定データを前記認証手段に提供する第４の工程と、

前記第１の認証鍵データを用いて、前記認証手段と前記認証を行う第５の工程と

を有する請求項６に記載のデータ処理方法。

８．　所定のデータを暗号化して認証先に出力するデータ処理装置であって、

認証鍵データおよび暗号鍵データを記憶する記憶手段と、

前記認証鍵データを用いて、認証先と認証を行う認証手段と、

前記認証手段の前記認証の後に、前記暗号鍵データを用いて所定のデータを暗号化する暗号化手段と、

前記暗号化手段の前記暗号化により得られたデータを前記認証先に出力する出力手段と

を有するデータ処理装置。

９．　認証鍵データおよび暗号鍵データを保持するデータ処理装置が実行するプログラムであって、

前記認証鍵データを用いて、認証先と認証を行う第１の手順と、

前記第１の手順の前記認証の後に、前記暗号鍵データを用いて所定のデータを暗号化する第２の手順と、

前記第２の手順の前記暗号化により得られたデータを前記認証先に出力する第３の手順と

を有するプログラム。

１０．　認証鍵データおよび復号鍵データを保持するデータ処理装置が行うデータ処理方法であって、

前記認証鍵データを用いて、被認証手段と認証を行う第１の工程と、

前記復号鍵データを用いて、前記被認証手段から受けたデータを復号する第２の工程と、

前記第１の工程の前記認証により前記被認証手段の正当性を認めると、前記第２の工程の前記復号により得られたデータを有効なものとして用いる第３

の工程と

を有するデータ処理方法。

１１．　所定の鍵データを保持する前記データ処理装置が、前記鍵データを用いて所定の生成手法で生成され前記鍵データを復元困難な第１の認証鍵データを保持する前記被認証手段と認証を行う場合に、

前記第１の工程は、

前記鍵データを指定する鍵指定データを前記被認証手段から受ける第４の工程と、

前記第４の工程で受けた前記鍵指定データが指定する前記鍵データを用いて前記所定の生成手法で第２の認証鍵データを生成する第５の工程と、

前記第５の工程で生成した前記第２の認証鍵データを用いて、前記第１の認証鍵データを前記認証に用いる前記被認証手段と前記認証を行う第６の工程と、

前記第６の工程の前記認証により、前記第１の認証用データと前記第２の認証用データとが同じであると判断した場合に、前記被認証手段の正当性を認める第７の工程と

を有する請求項１０に記載のデータ処理方法。

１２．　前記第３の工程において、前記鍵データに関連付けられた、前記被認証手段に許可されたデータ処理装置の機能、または前記データ処理装置が保持するデータへのアクセスを実行する

請求項１０に記載のデータ処理方法。

１３．　認証鍵データおよび復号鍵データを保持するデータ処理装置であって、

前記認証鍵データを用いて、被認証手段と認証を行う認証手段と、

前記被認証手段からデータを入力する入力手段と、

前記復号鍵データを用いて、前記入力手段を介して前記被認証手段から入力した前記データを復号する復号手段と、

前記認証手段の前記認証により前記被認証手段の正当性を認めると、前記復号手段の前記復号により得られたデータを有効なものとして用いる制御手段と

を有するデータ処理装置。

１４．　認証鍵データおよび復号鍵データを保持するデータ処理装置が実行するプログラムであって、

前記認証鍵データを用いて、被認証手段と認証を行う第１の手順と、

前記復号鍵データを用いて、前記被認証手段から受けたデータを復号する第２の手順と、

前記第１の手順の前記認証により前記被認証手段の正当性を認めると、前記第２の手順の前記復号により得られたデータを有効なものとして用いる第３の手順と

を有するプログラム。

FIG. 1

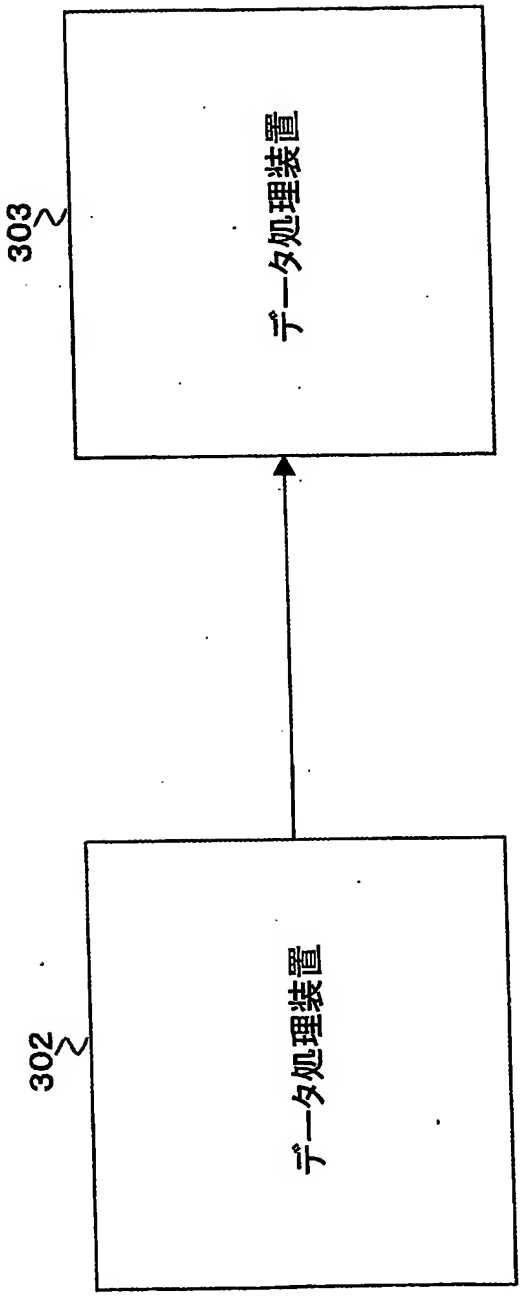


FIG. 2

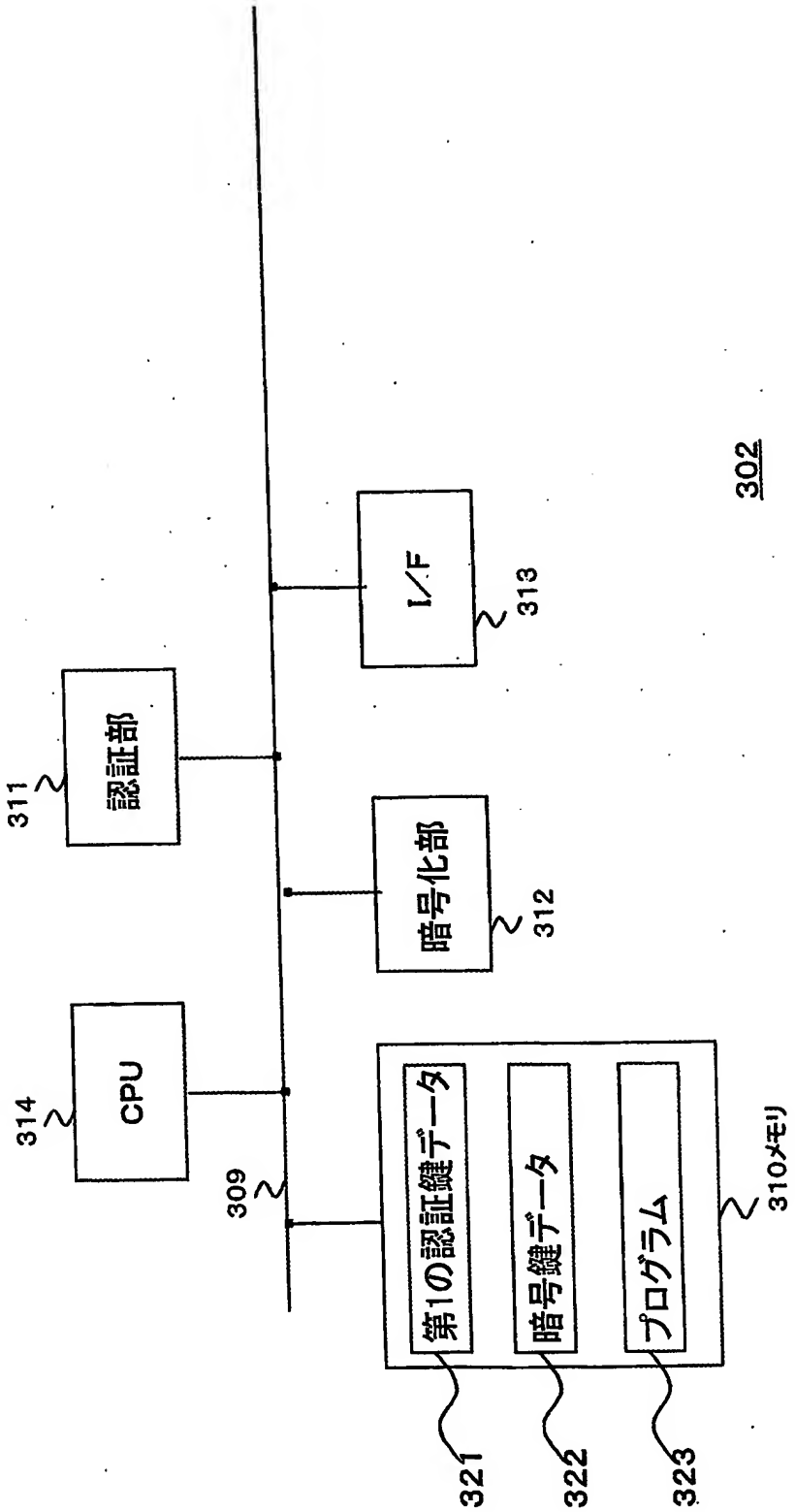

302
I/F
313
認証部
311
暗号化部
312
CPU
314
309
第1の認証鍵データ
暗号鍵データ
プログラム
310メモリ
321
322
323

FIG. 3

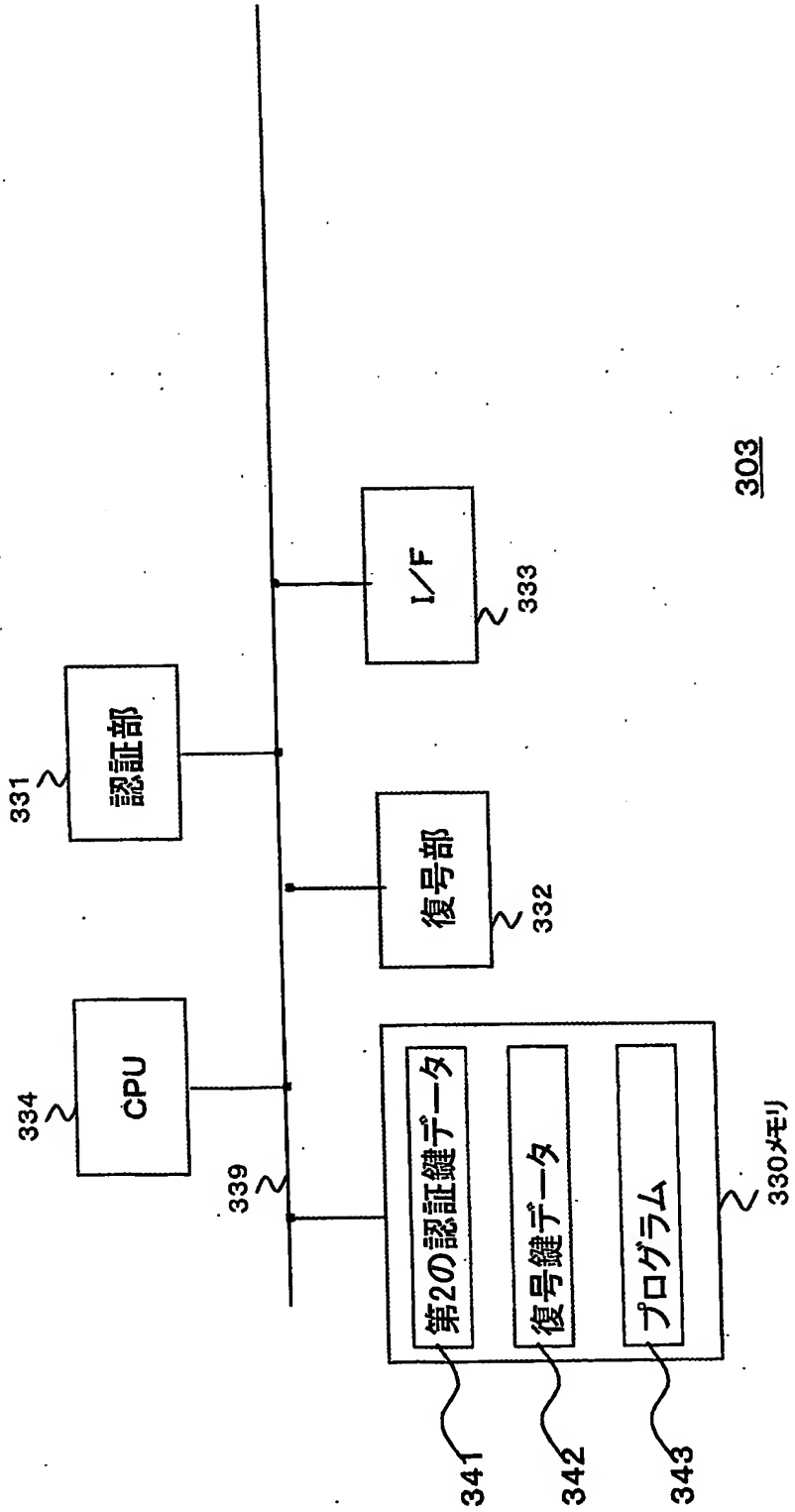

303
I/F
333
認証部
331
復号部
332
CPU
334
339
第2の認証鍵データ
復号鍵データ
プログラム
330メモリ
341
342
343

FIG. 4

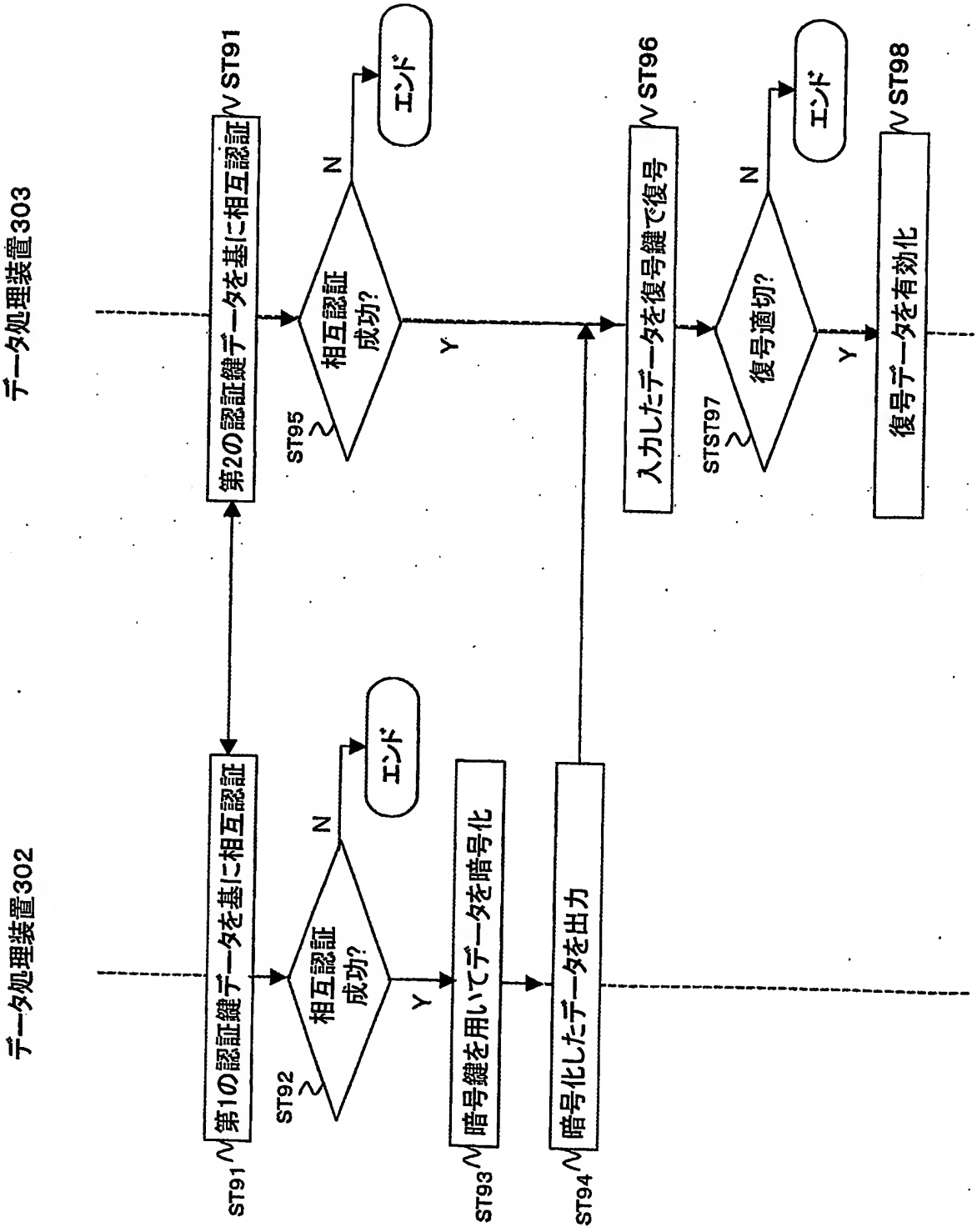

データ処理装置302
データ処理装置303
第1の認証鍵データを基に相互認証
ST91
相互認証成功?
ST92
N
Y
エンド
暗号鍵を用いてデータを暗号化
ST93
暗号化したデータを出力
ST94
第2の認証鍵データを基に相互認証
ST91
相互認証成功?
ST95
N
Y
エンド
入力したデータを復号鍵で復号
ST96
復号適切?
STST97
N
Y
エンド
復号データを有効化
ST98

FIG. 5

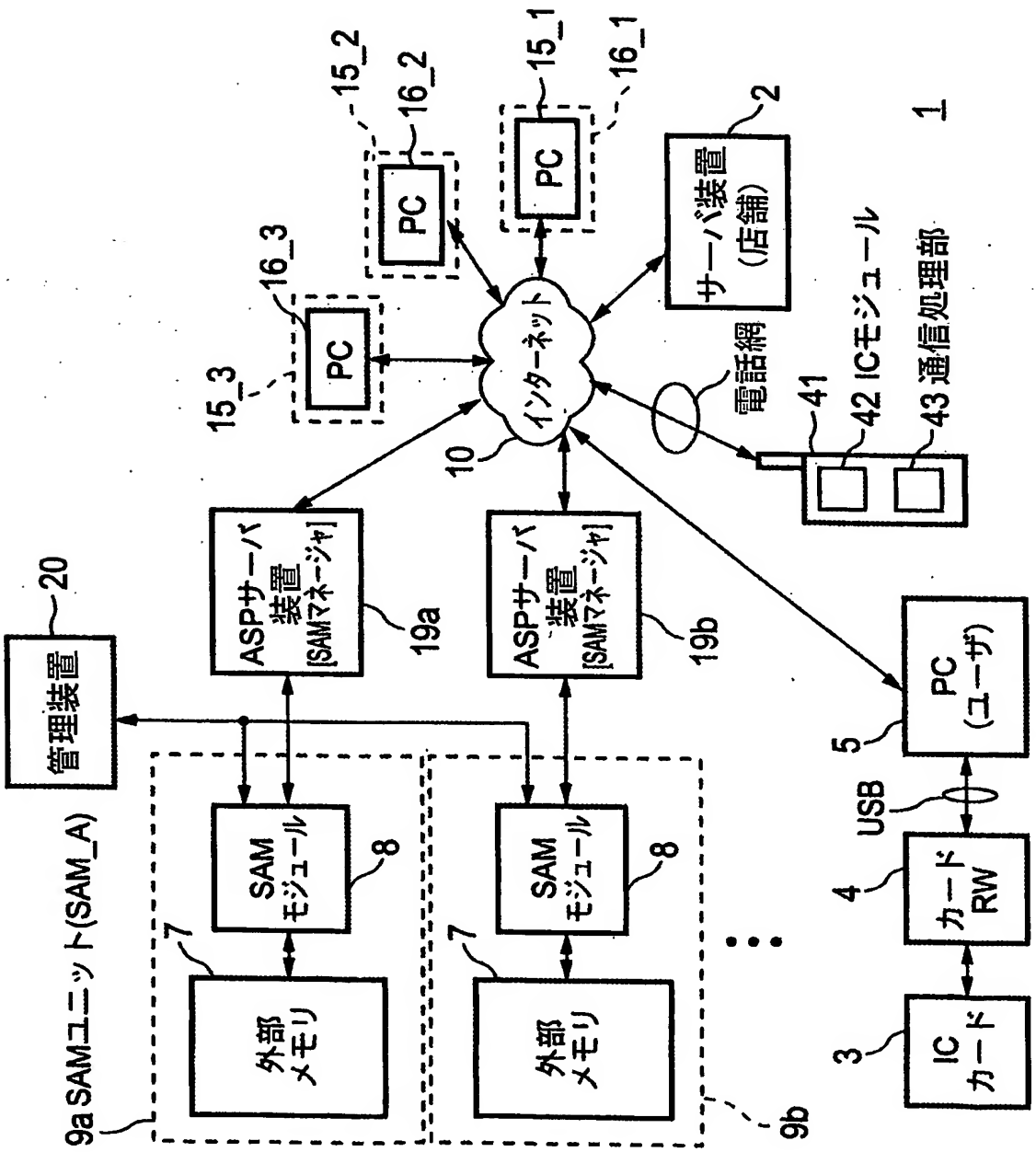

1
2
サーバ装置
(店舗)
15_1
16_1
PC
15_2
16_2
PC
15_3
16_3
PC
インターネット
10
電話網
41
42 ICモジュール
43 通信処理部
ASPサーバ
装置
[SAMマネージャ]
19a
ASPサーバ
装置
[SAMマネージャ]
19b
20
管理装置
PC
(ユーザ)
5
USB
4
カード
RW
3
IC
カード
SAM
モジュール
8
7
外部
メモリ
9a SAMユニット(SAM_A)
9b

FIG. 6

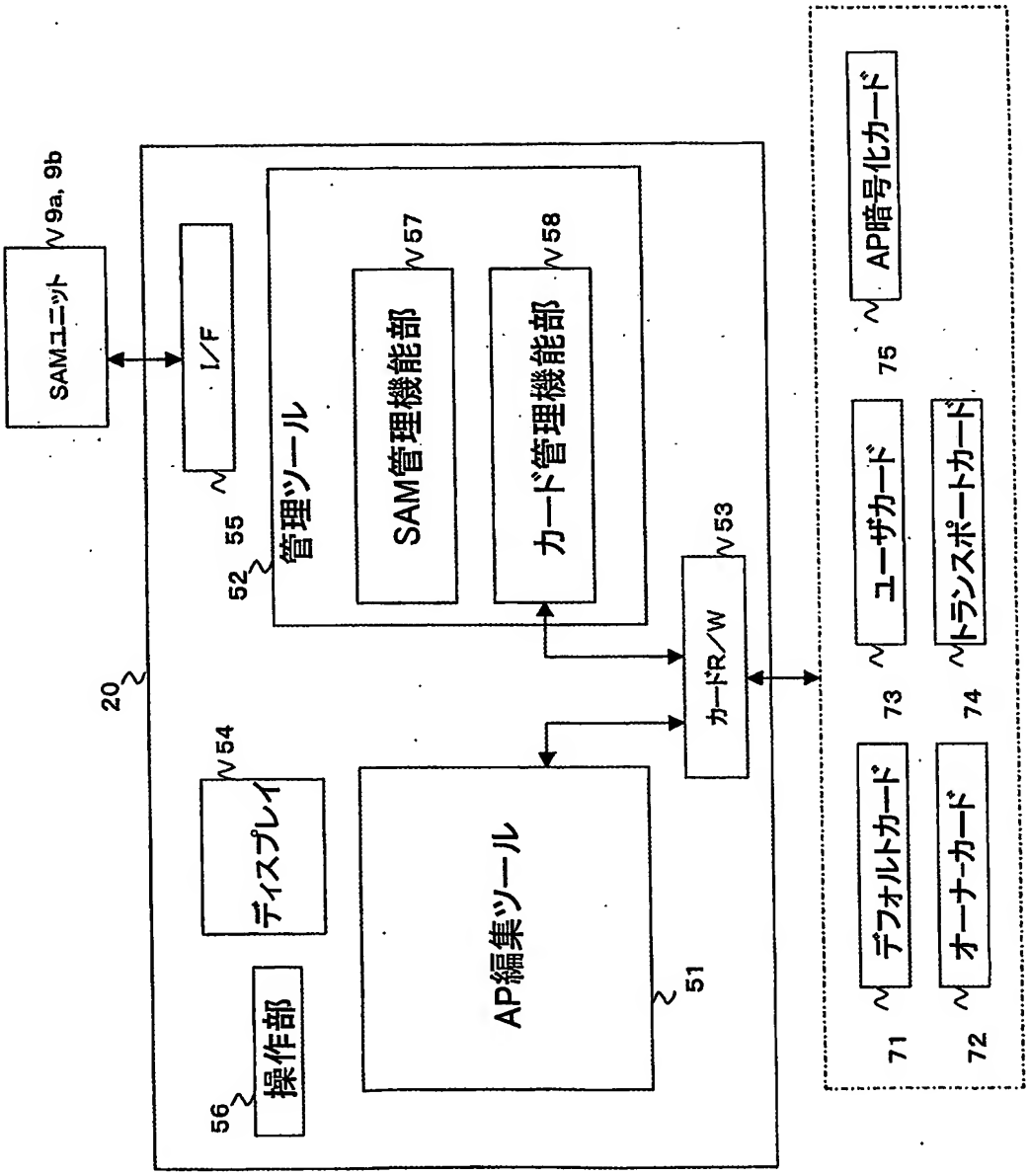

SAMユニット
9a, 9b
I/F
55
管理ツール
52
SAM管理機能部
57
カード管理機能部
58
カードR/W
53
20
ディスプレイ
54
操作部
56
AP編集ツール
51
AP暗号化カード
75
ユーザカード
73
トランスポートカード
74
デフォルトカード
71
オーナーカード
72

FIG. 7

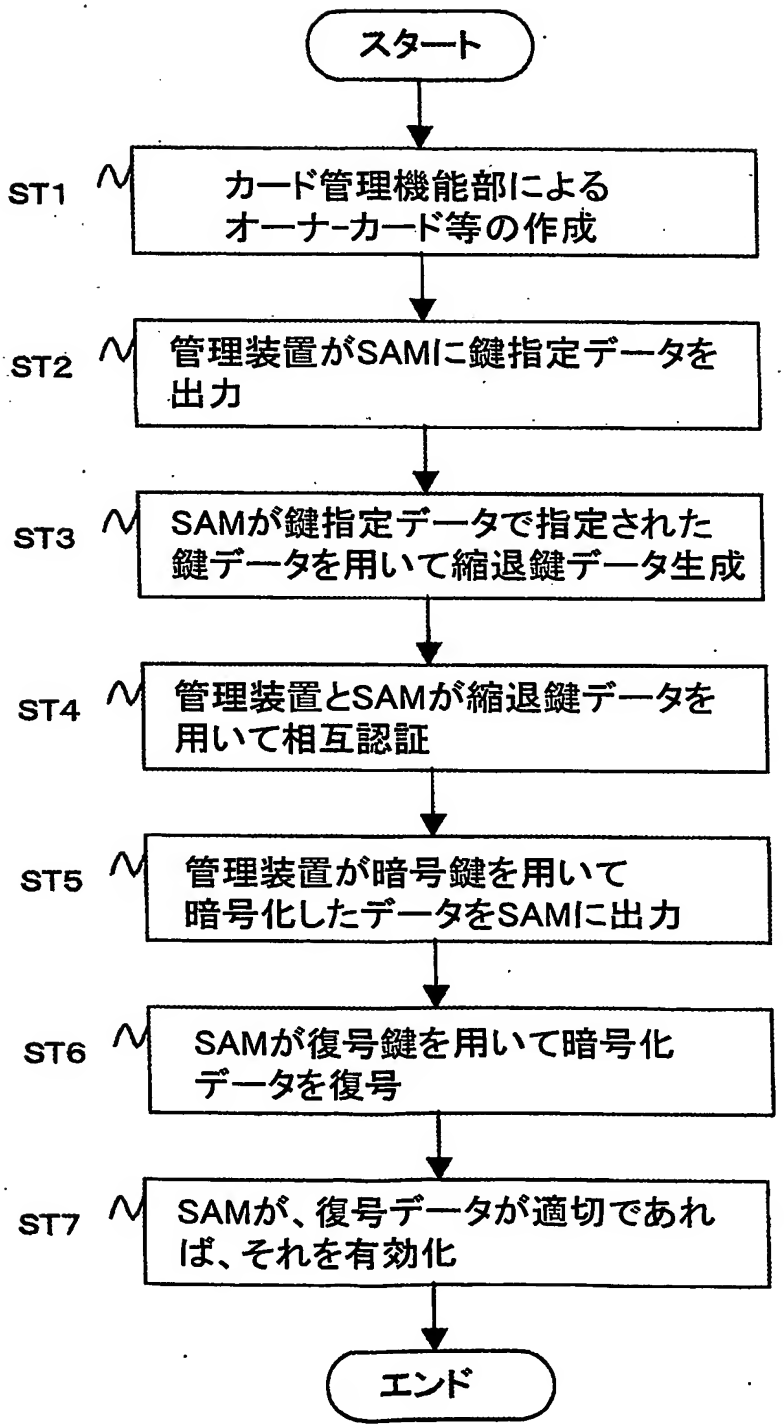

スタート
ST1
カード管理機能部による
オーナーカード等の作成
ST2
管理装置がSAMに鍵指定データを
出力
ST3
SAMが鍵指定データで指定された
鍵データを用いて縮退鍵データ生成
ST4
管理装置とSAMが縮退鍵データを
用いて相互認証
ST5
管理装置が暗号鍵を用いて
暗号化したデータをSAMに出力
ST6
SAMが復号鍵を用いて暗号化
データを復号
ST7
SAMが、復号データが適切であれ
ば、それを有効化
エンド

FIG. 8

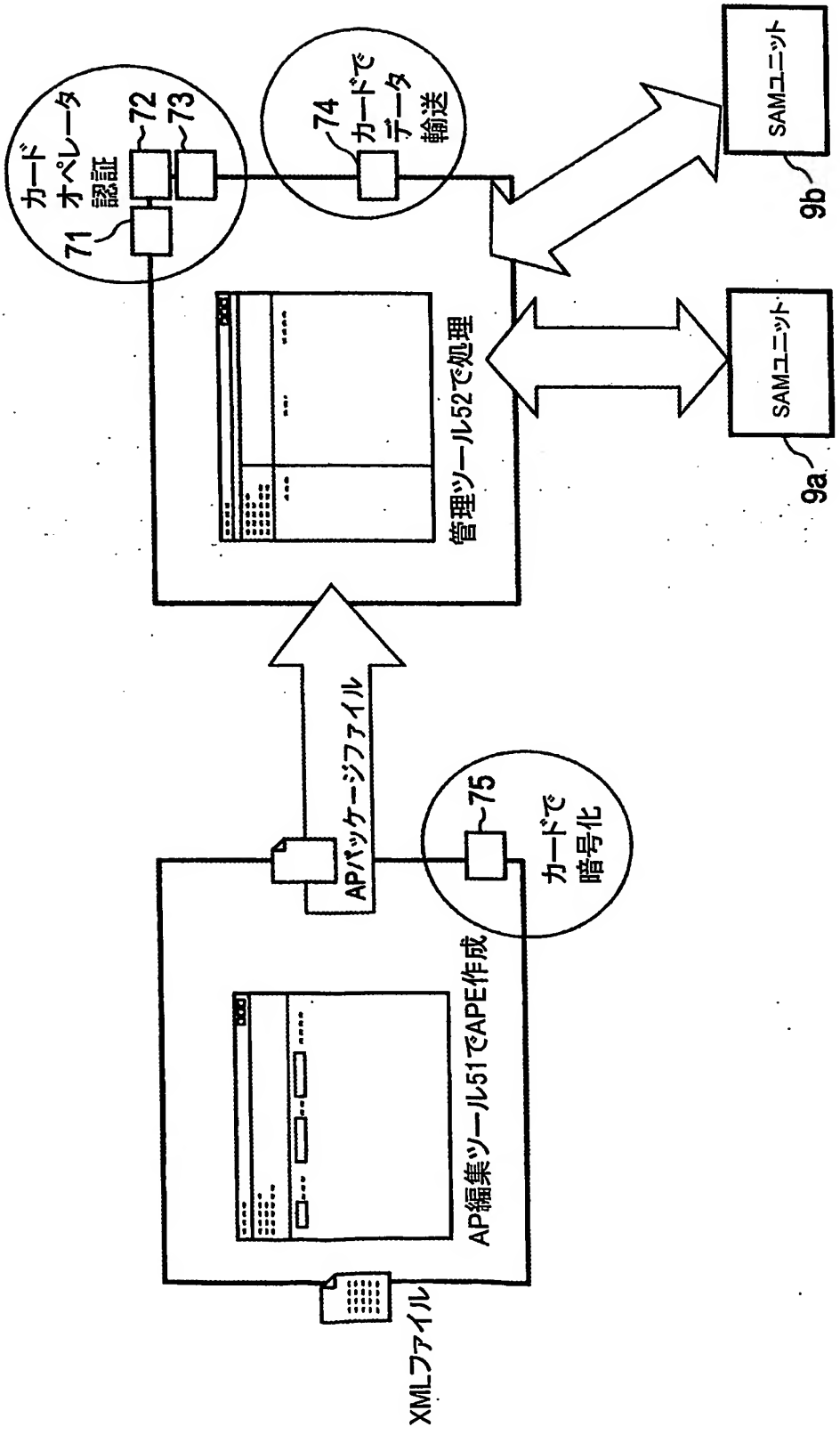

カード
オペレータ
認証
71
72
73
74
カードで
データ
輸送
SAMユニット
9b
SAMユニット
9a
管理ツール52で処理
APパッケージファイル
75
カードで
暗号化
AP編集ツール51でAPE作成
XMLファイル

FIG. 9

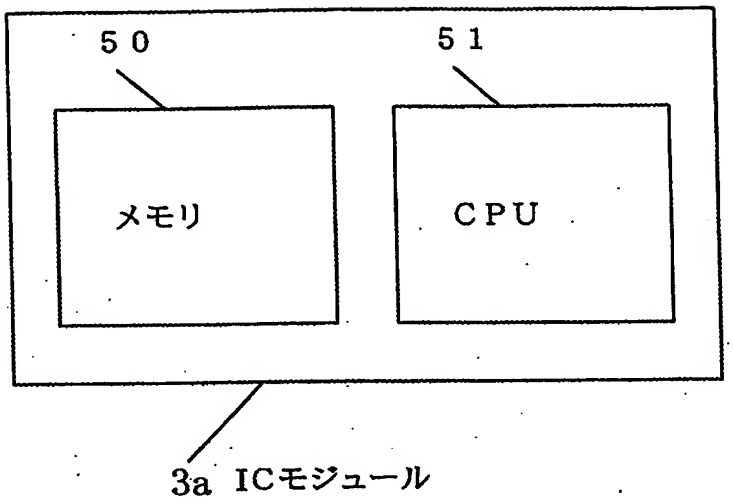

５０
５１
メモリ
ＣＰＵ
3a ICモジュール

FIG. 10

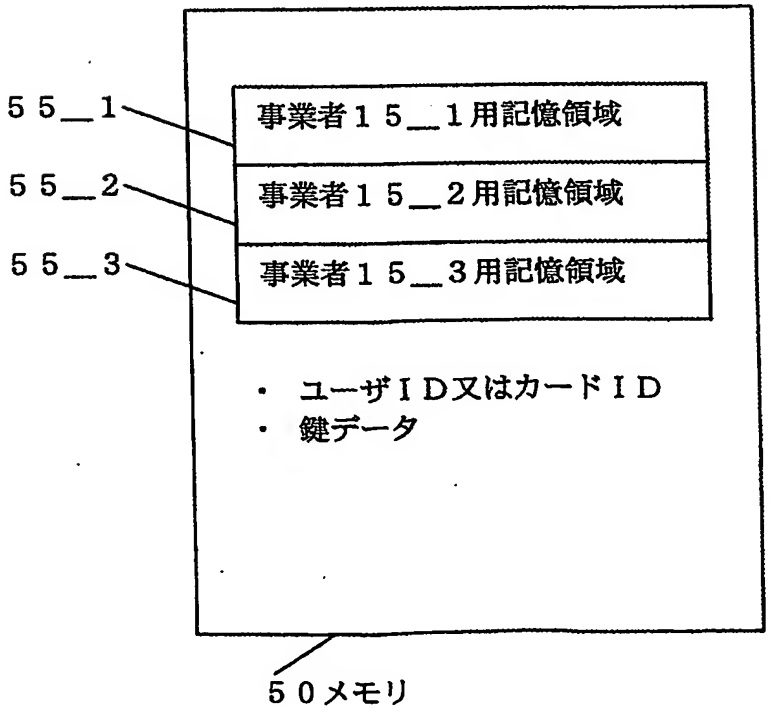

５５＿１
５５＿２
５５＿３
事業者１５＿１用記憶領域
事業者１５＿２用記憶領域
事業者１５＿３用記憶領域
・ ユーザＩＤ又はカードＩＤ
・ 鍵データ
５０メモリ

FIG. 11

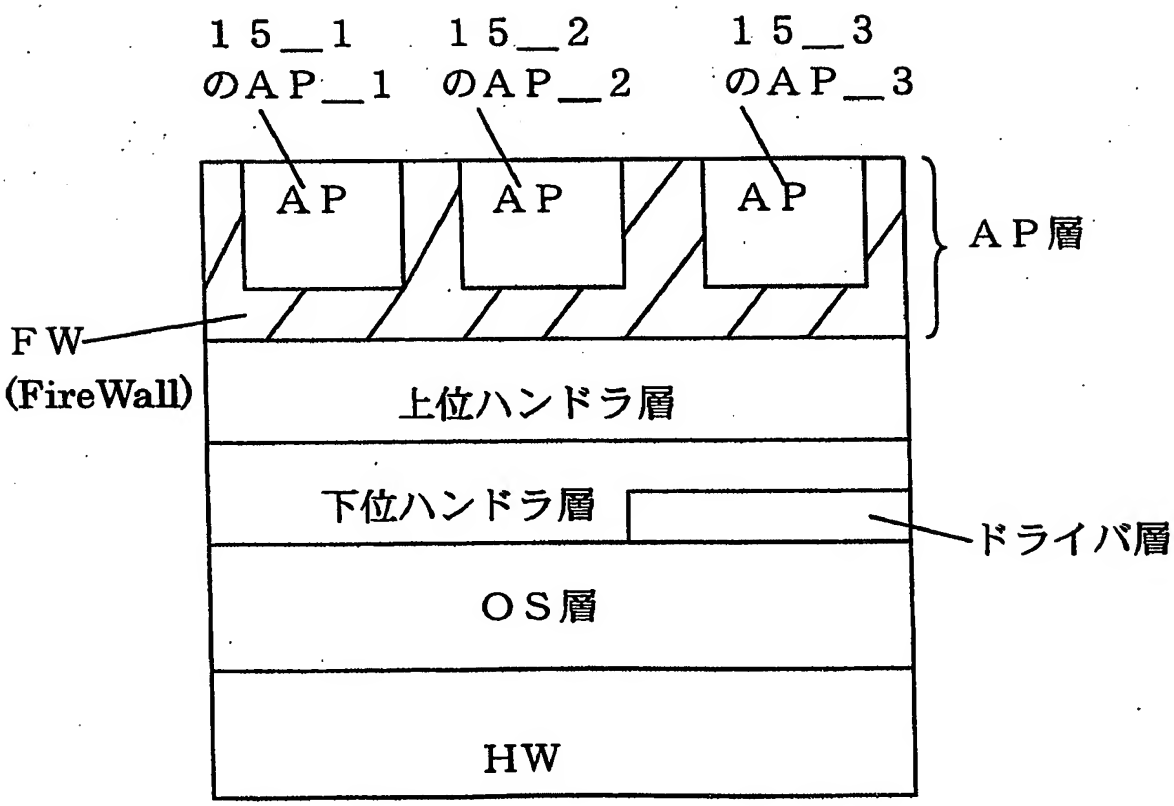

１５＿１
のＡＰ＿１
１５＿２
のＡＰ＿２
１５＿３
のＡＰ＿３
ＡＰ
ＡＰ
ＡＰ
ＡＰ層
ＦＷ
(FireWall)
上位ハンドラ層
下位ハンドラ層
ドライバ層
ＯＳ層
HW

FIG. 12

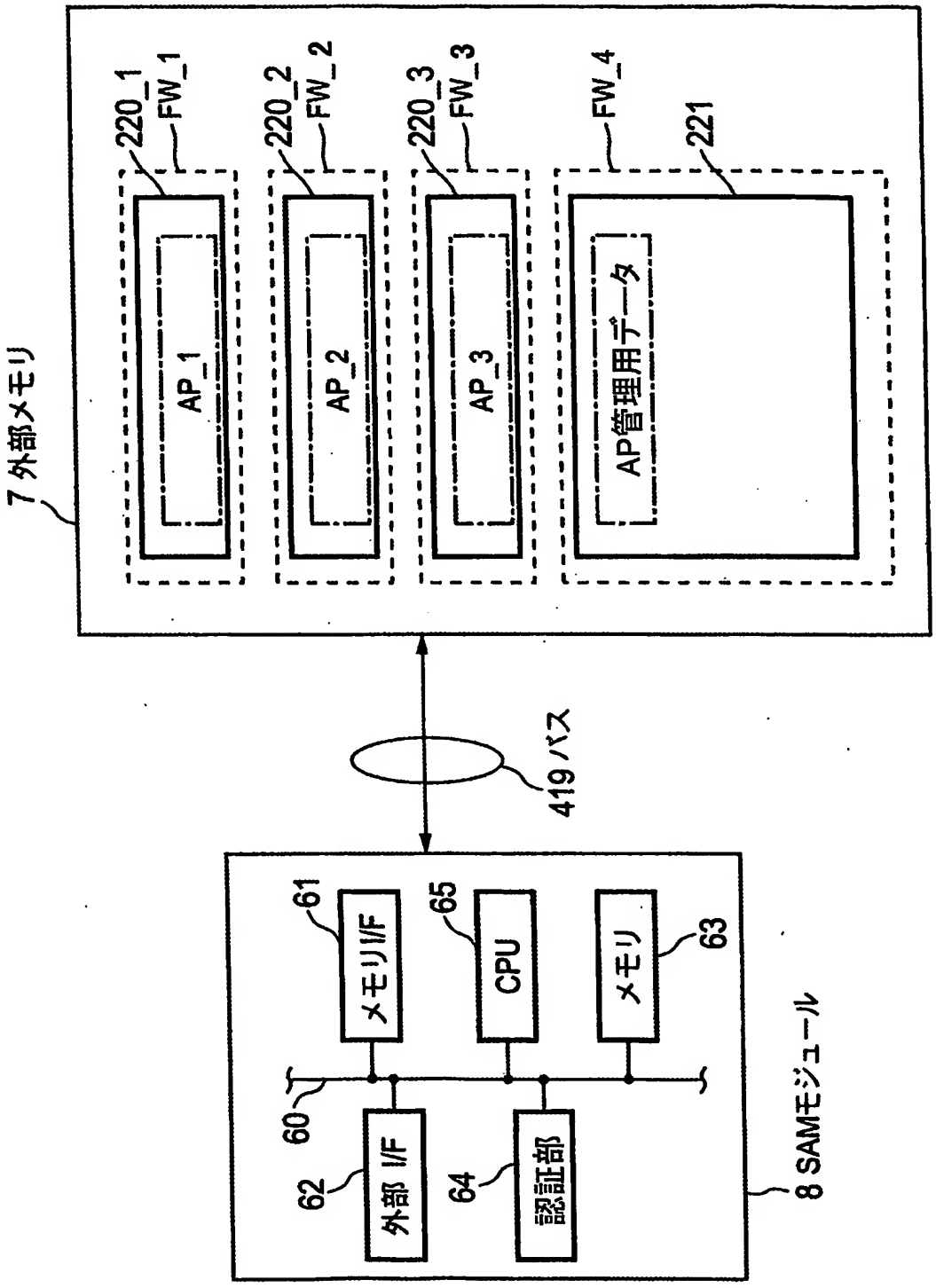

7 外部メモリ
220_1
FW_1
AP_1
220_2
FW_2
AP_2
220_3
FW_3
AP_3
FW_4
221
AP管理用データ
419 バス
61
メモリI/F
65
CPU
63
メモリ
60
62
外部 I/F
64
認証部
8 SAMモジュール

FIG. 13

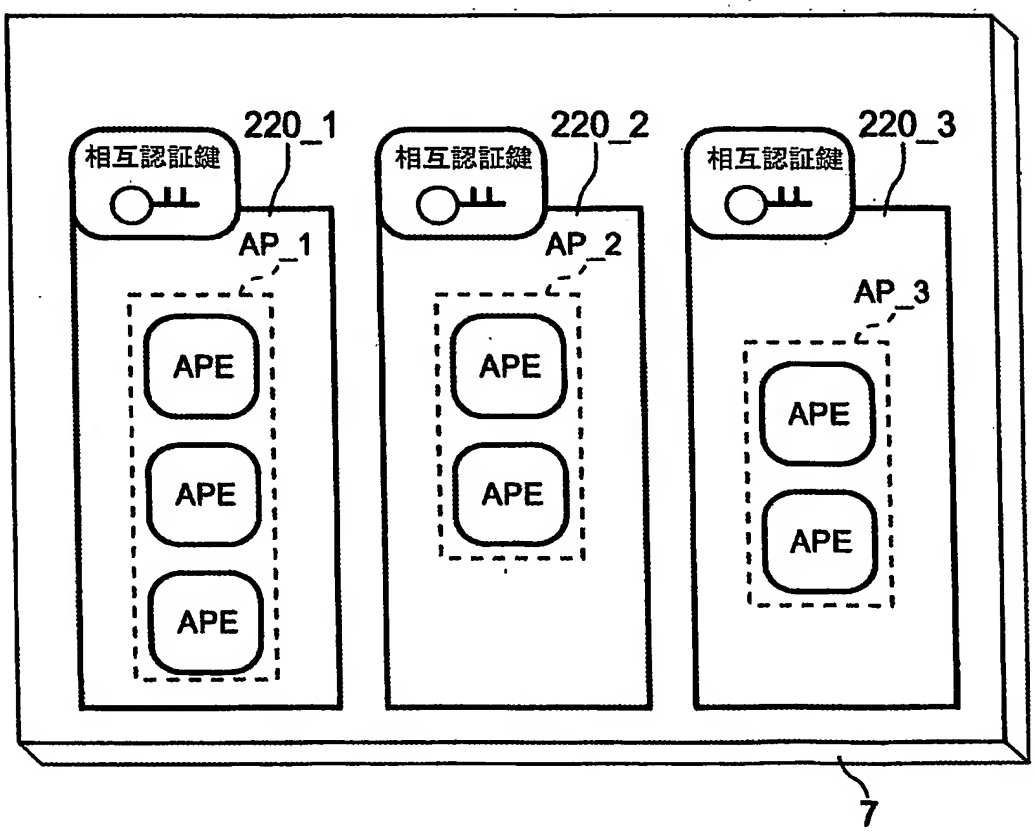

220_1
相互認証鍵
AP_1
APE
APE
APE
220_2
相互認証鍵
AP_2
APE
APE
220_3
相互認証鍵
AP_3
APE
APE
7

FIG. 14

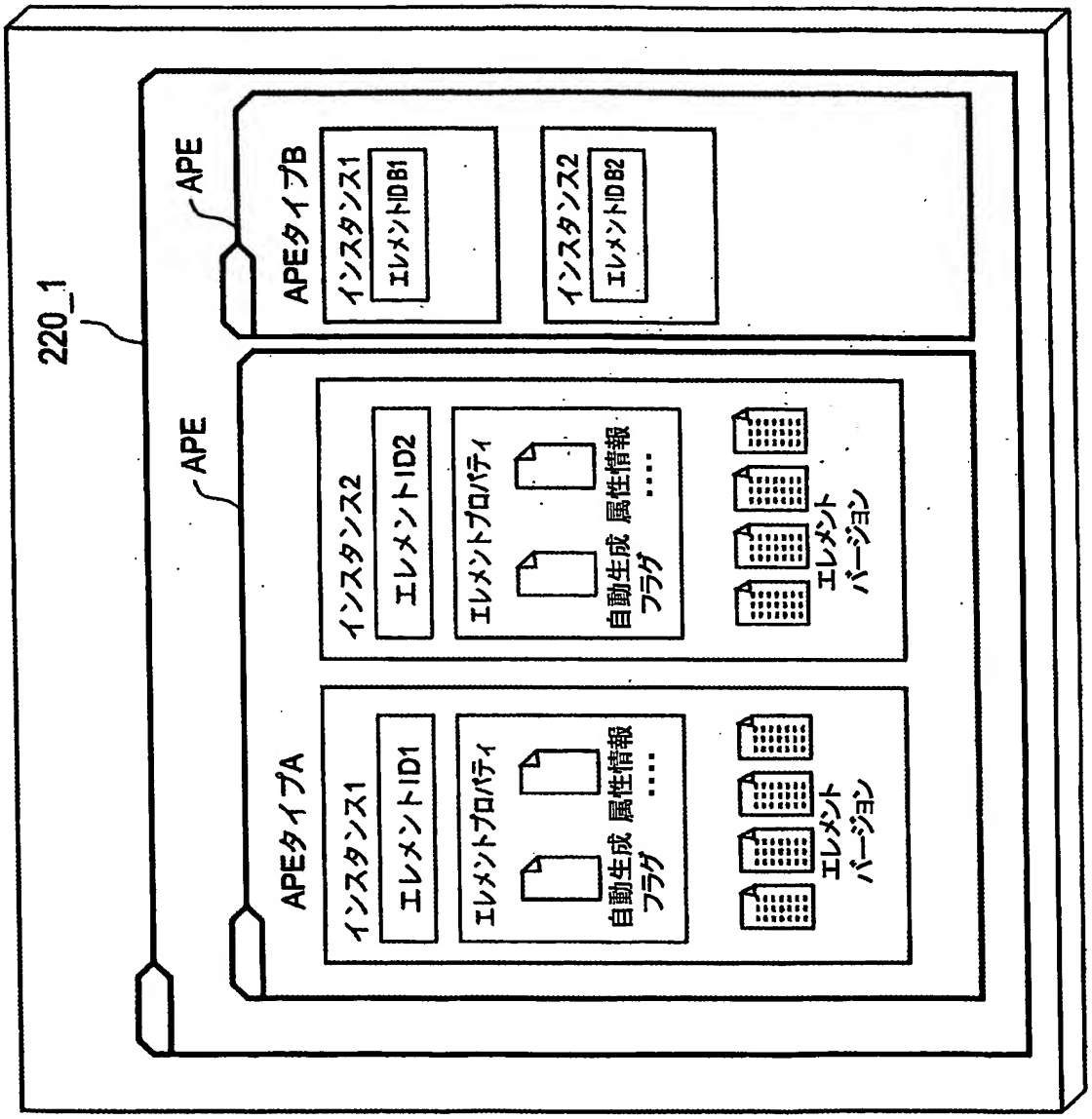

220_1
APE
APEタイプB
インスタンス1
エレメントID B1
インスタンス2
エレメントID B2
APE
APEタイプA
インスタンス1
エレメントID1
エレメントプロパティ
自動生成 属性情報 フラグ ....
エレメント バージョン
インスタンス2
エレメントID2
エレメントプロパティ
自動生成 属性情報 フラグ ....
エレメント バージョン

FIG. 15

APE タイプ番号	APEタイプ
・・・	ICシステム鍵
・・・	ICエリア鍵
・・・	ICサービス鍵
・・・	IC縮退鍵
・・・	IC鍵変更パッケージ
・・・	IC発行鍵パッケージ
・・・	IC拡張発行鍵パッケージ
・・・	ICエリア登録鍵パッケージ
・・・	ICエリア削除鍵パッケージ
・・・	ICサービス登録鍵パッケージ
・・・	ICサービス削除鍵パッケージ
・・・	ICメモリ分割鍵パッケージ
・・・	ICメモリ分割素鍵パッケージ
・・・	障害記録ファイル
・・・	相互認証用鍵
・・・	パッケージ鍵
・・・	ネガリスト
・・・	サービスデータテンポラリファイル

FIG. 16

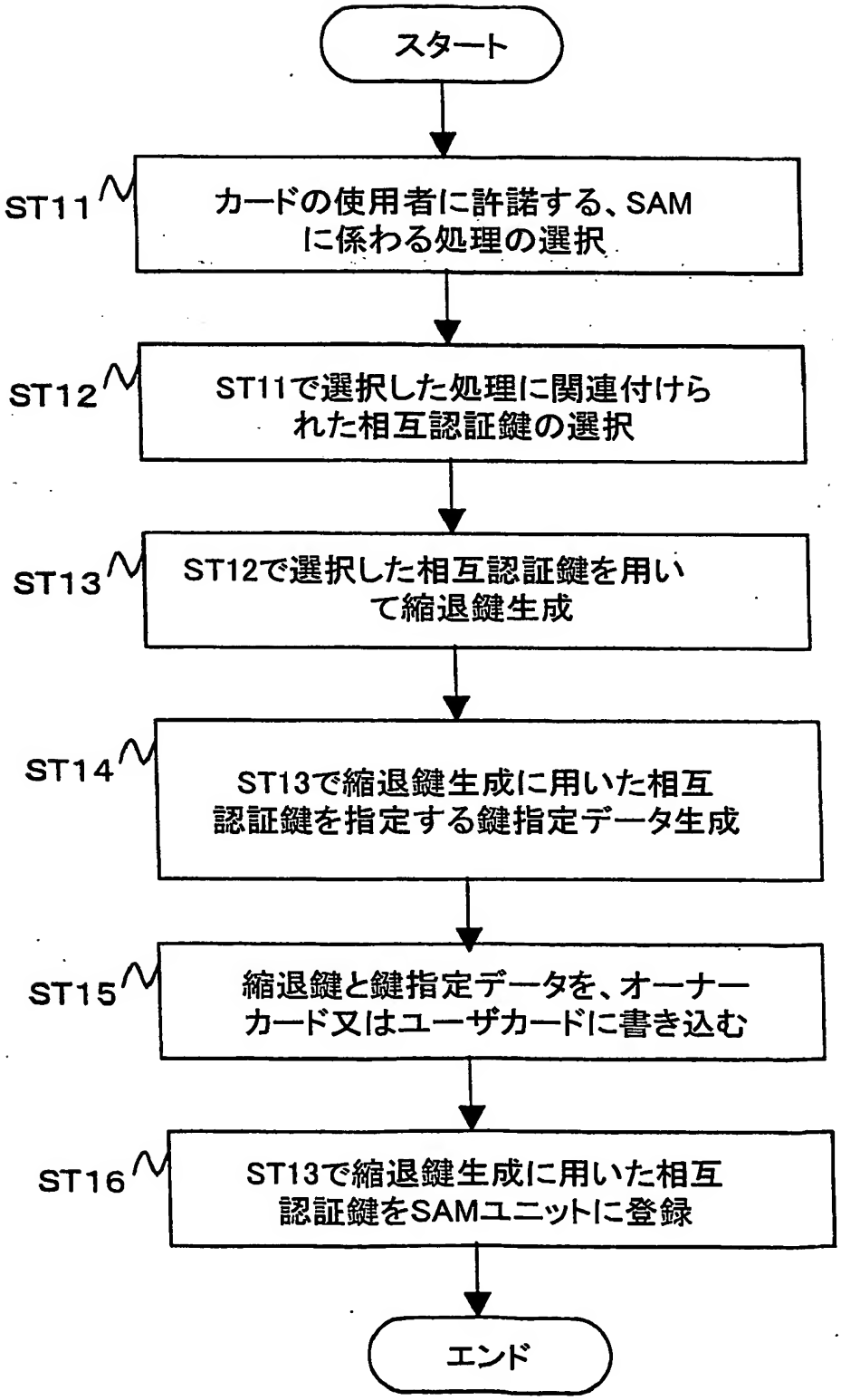

スタート
ST11
カードの使用者に許諾する、SAMに係わる処理の選択
ST12
ST11で選択した処理に関連付けられた相互認証鍵の選択
ST13
ST12で選択した相互認証鍵を用いて縮退鍵生成
ST14
ST13で縮退鍵生成に用いた相互認証鍵を指定する鍵指定データ生成
ST15
縮退鍵と鍵指定データを、オーナーカード又はユーザカードに書き込む
ST16
ST13で縮退鍵生成に用いた相互認証鍵をSAMユニットに登録
エンド

FIG. 17

相互認証鍵名	AP記憶領域・ID	APEタイプ番号	インスタンス番号	エレメントバージョン
デバイス鍵	...	...	...	...
ターミネーション鍵	...	...	...	...
製造設定サービス相互認証鍵	...	...	...	...
機器管理サービス相互認証鍵	...	...	...	...
通信管理サービス相互認証鍵	...	...	...	...
相互認証サービス相互認証鍵	...	...	...	...
AP記憶領域管理サービス相互認証鍵	...	...	...	...
サービスAP・記憶領域相互認証鍵	...	...	...	...
システムAP・記憶領域相互認証鍵	...	...	...	...
製造者AP記憶領域相互認証鍵	...	...	...	...

FIG. 18

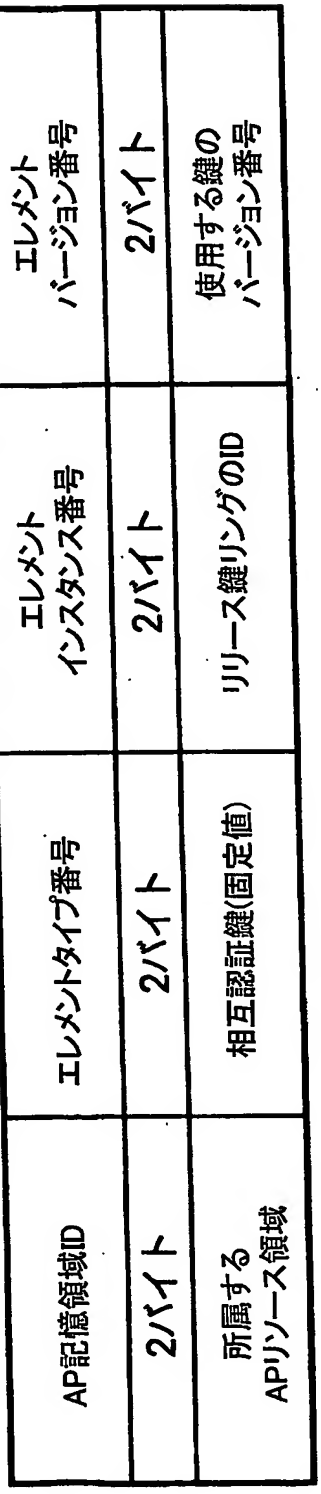

AP記憶領域ID
エレメントタイプ番号
エレメント
インスタンス番号
エレメント
バージョン番号
2バイト
2バイト
2バイト
2バイト
所属する
APリソース領域
相互認証鍵(固定値)
リリース鍵リングのID
使用する鍵の
バージョン番号

FIG. 19A

相互認証鍵名	AP記憶領域ID	APE タイプ番号	インスタンス番号	エレメント バージョン番号
デバイス鍵	・・・	・・・	・・・	・・・
機器管理サービス相互認証鍵	・・・	・・・	・・・	・・・
通信管理サービス相互認証鍵	・・・	・・・	・・・	・・・
AP記憶領域管理 サービス相互認証鍵	・・・	・・・	・・・	・・・
サービスAP記憶領域 AP-R相互認証鍵	・・・	・・・	・・・	・・・
ターミネーション鍵	・・・	・・・	・・・	・・・

FIG. 19B

・実行可能なコマンド

サービス種別	コマンド名
機器管理サービス	・・・
通信管理サービス	・・・
ICサービス	・・・
相互認証サービス	・・・
AP記憶領域管理サービス	・・・

FIG. 20

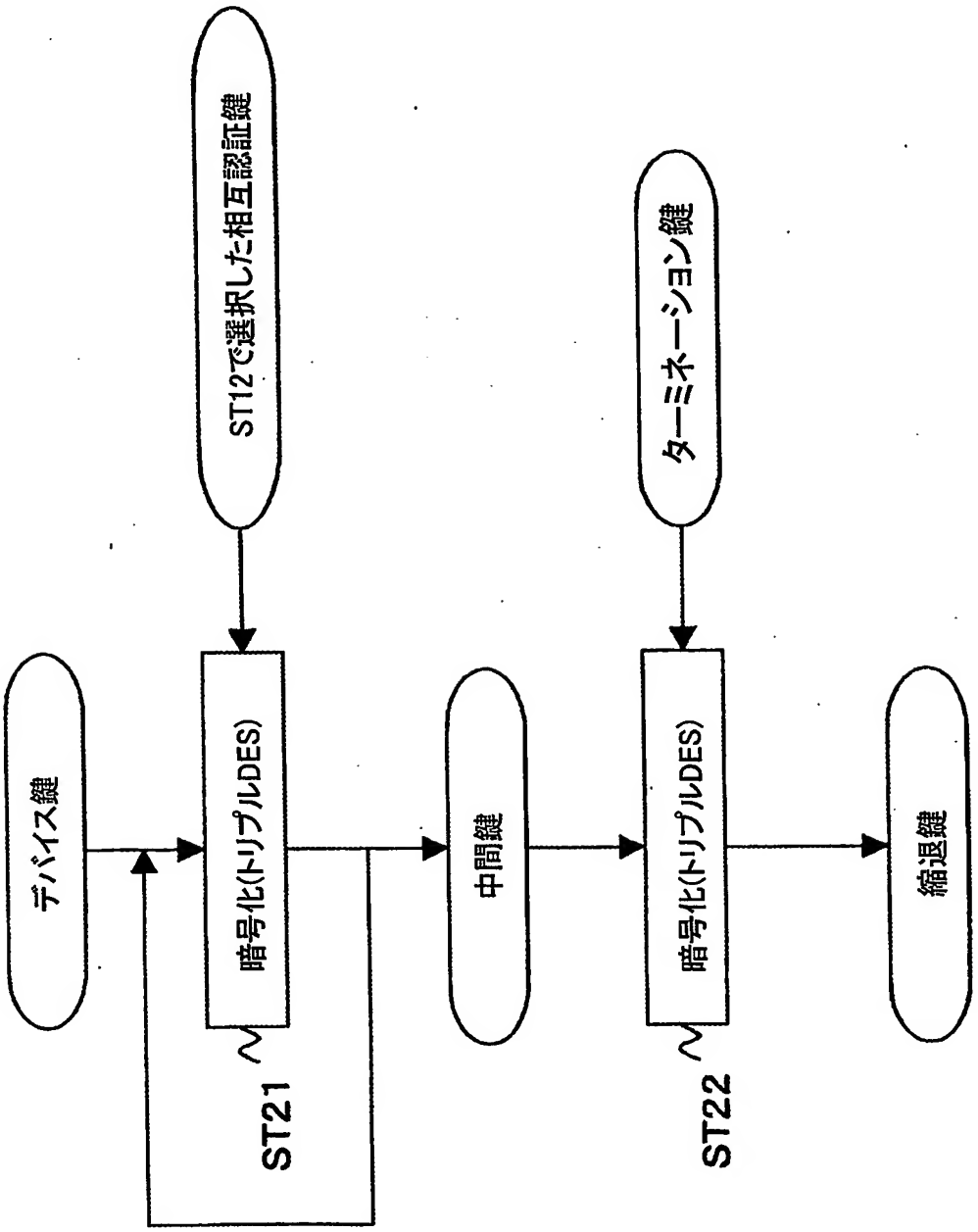

ST12で選択した相互認証鍵
ターミネーション鍵
デバイス鍵
暗号化(トリプルDES)
中間鍵
暗号化(トリプルDES)
縮退鍵
ST21
ST22

FIG. 21

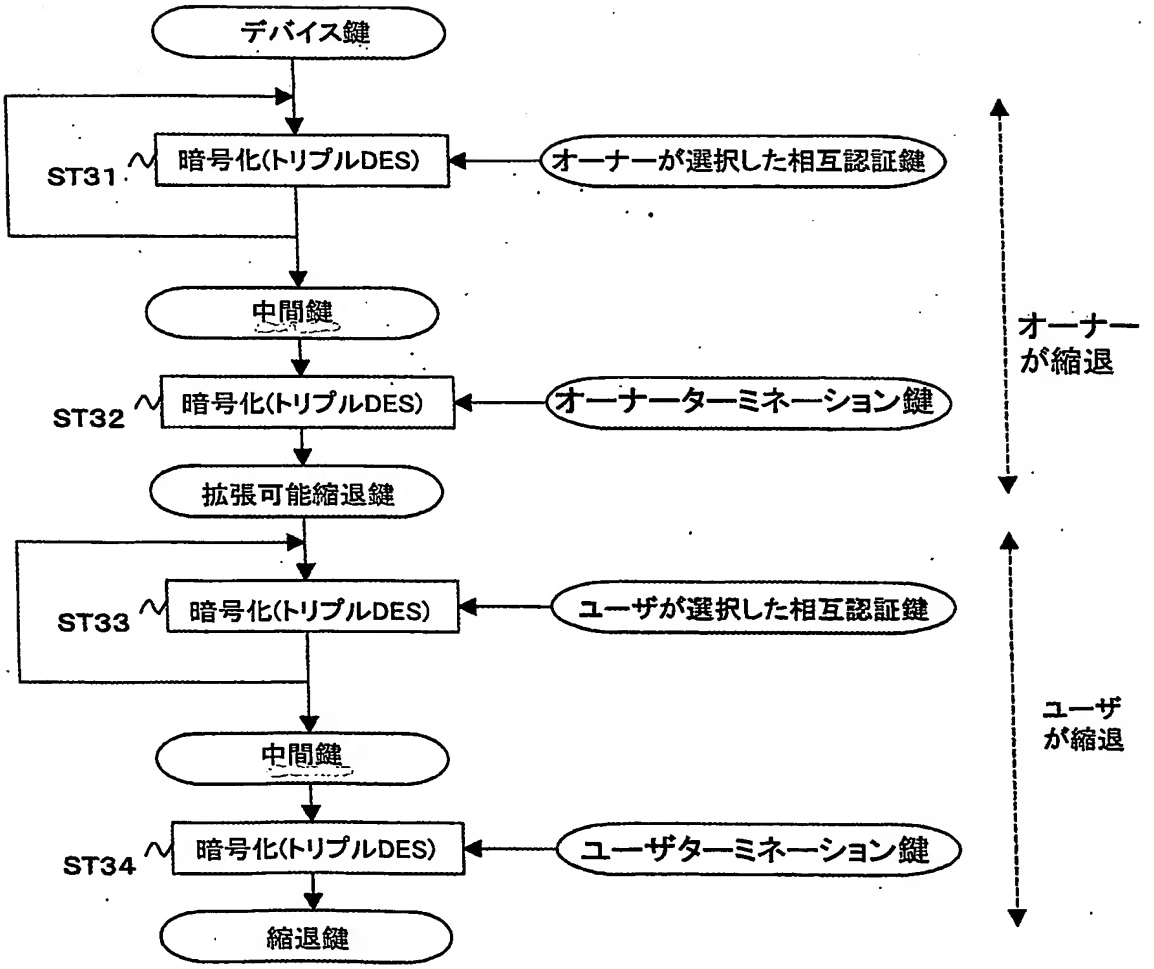

デバイス鍵
ST31
暗号化(トリプルDES)
オーナーが選択した相互認証鍵
中間鍵
ST32
暗号化(トリプルDES)
オーナーターミネーション鍵
拡張可能縮退鍵
ST33
暗号化(トリプルDES)
ユーザが選択した相互認証鍵
中間鍵
ST34
暗号化(トリプルDES)
ユーザターミネーション鍵
縮退鍵
オーナーが縮退
ユーザが縮退

FIG. 22

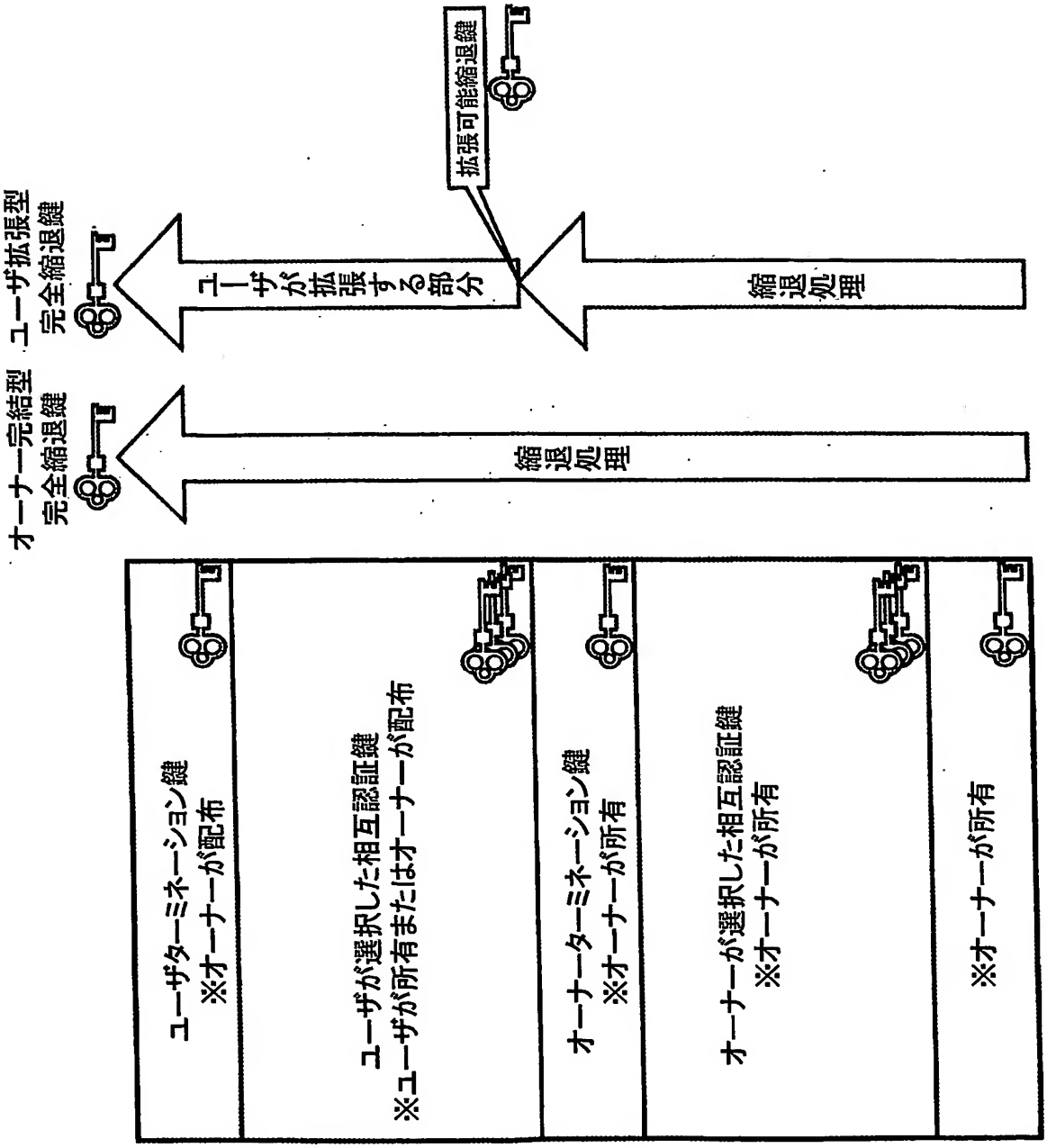

ユーザ拡張型
完全縮退鍵
拡張可能縮退鍵
ユーザが拡張する部分
縮退処理
オーナー完結型
完全縮退鍵
縮退処理
ユーザターミネーション鍵
※オーナーが配布
ユーザが選択した相互認証証鍵
※ユーザが所有またはオーナーが配布
オーナーターミネーション鍵
※オーナーが所有
オーナーが選択した相互認証証鍵
※オーナーが所有
※オーナーが所有

FIG. 23

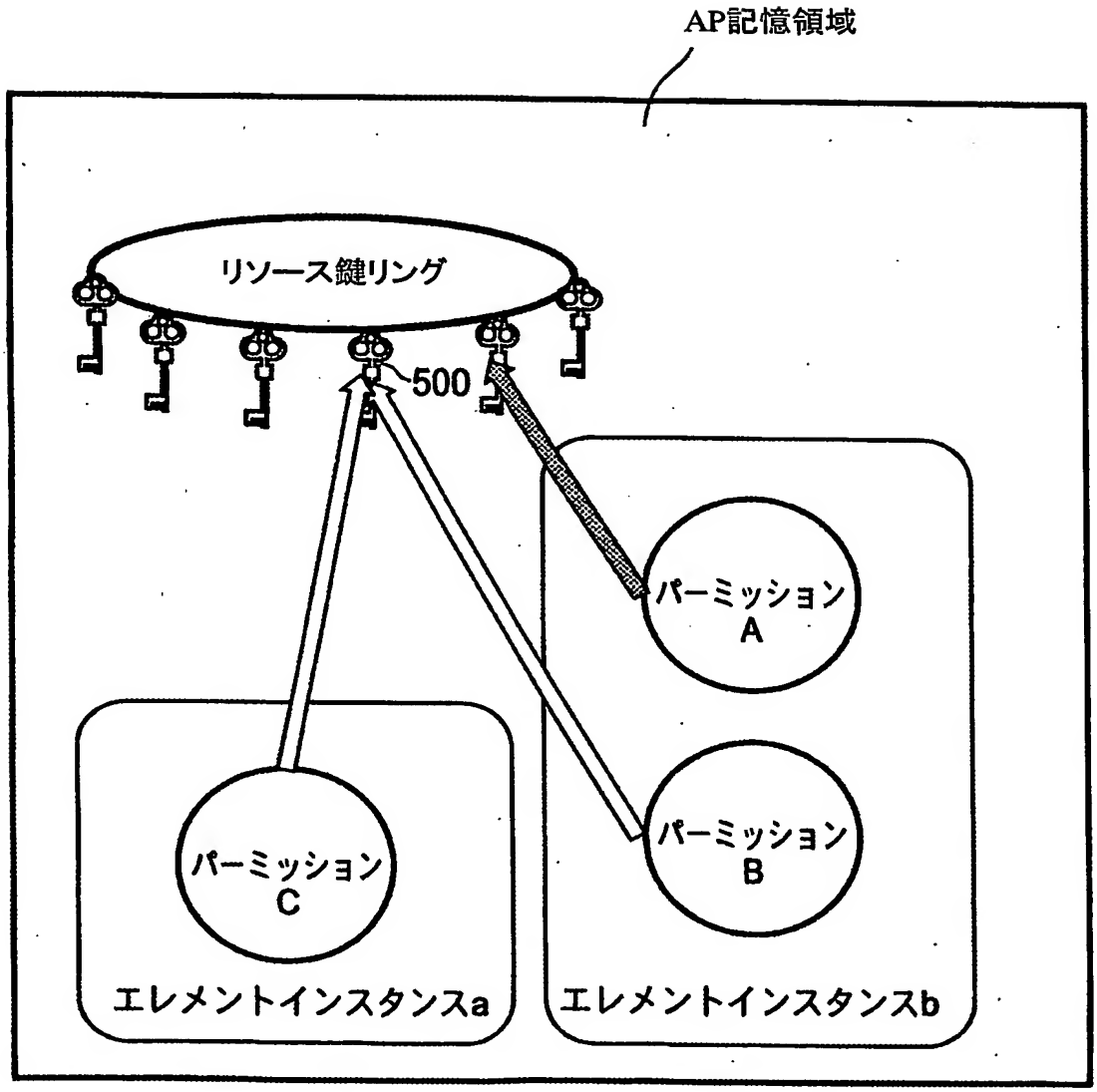

AP記憶領域
リソース鍵リング
500
パーミッション A
パーミッション B
パーミッション C
エレメントインスタンスa
エレメントインスタンスb

FIG. 24

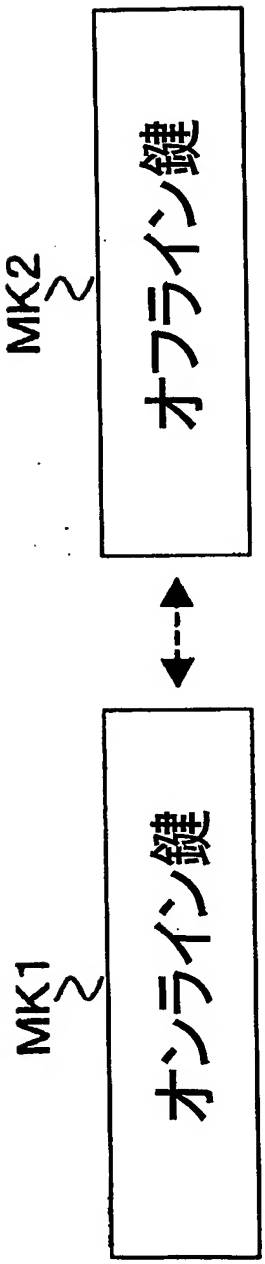


FIG. 25

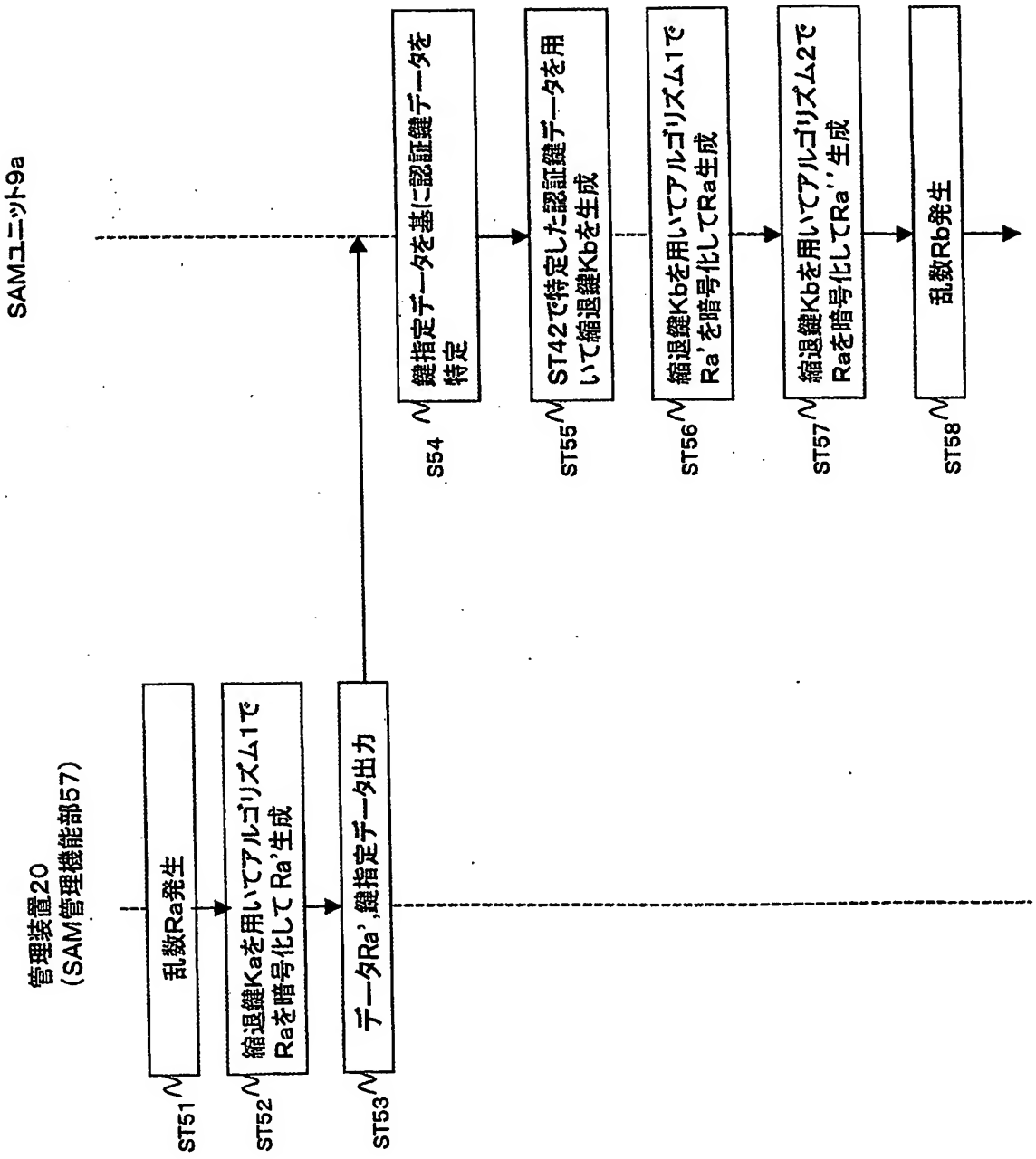

管理装置20
(SAM管理機能部57)
SAMユニット9a
乱数Ra発生
縮退鍵Kaを用いてアルゴリズム1でRaを暗号化してRa'生成
データRa',鍵指定データ出力
鍵指定データを基に認証鍵データを特定
ST42で特定した認証鍵データを用いて縮退鍵Kbを生成
縮退鍵Kbを用いてアルゴリズム1でRa'を暗号化してRa生成
縮退鍵Kbを用いてアルゴリズム2でRaを暗号化してRa''生成
乱数Rb発生
ST51
ST52
ST53
S54
ST55
ST56
ST57
ST58

FIG. 26

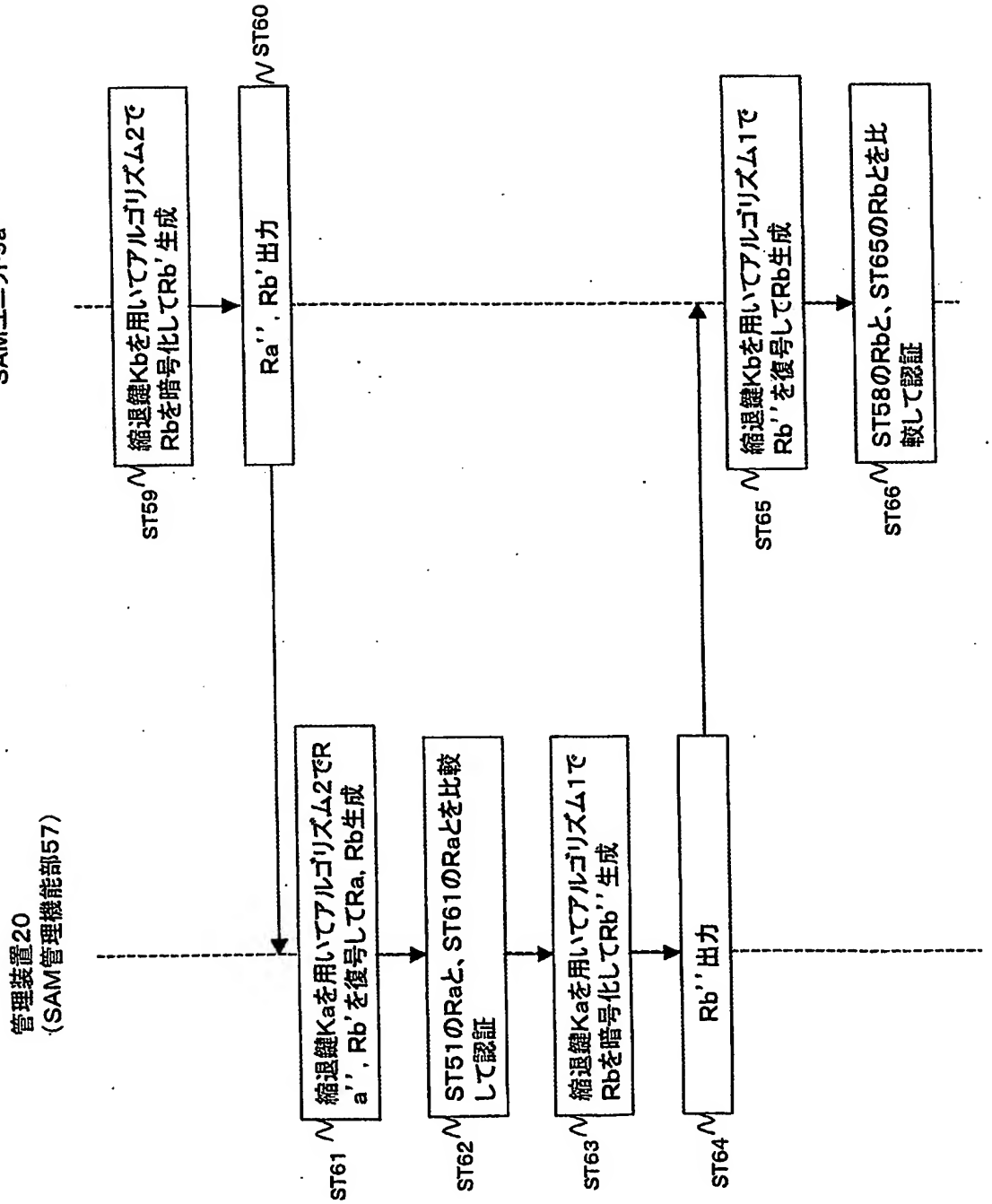
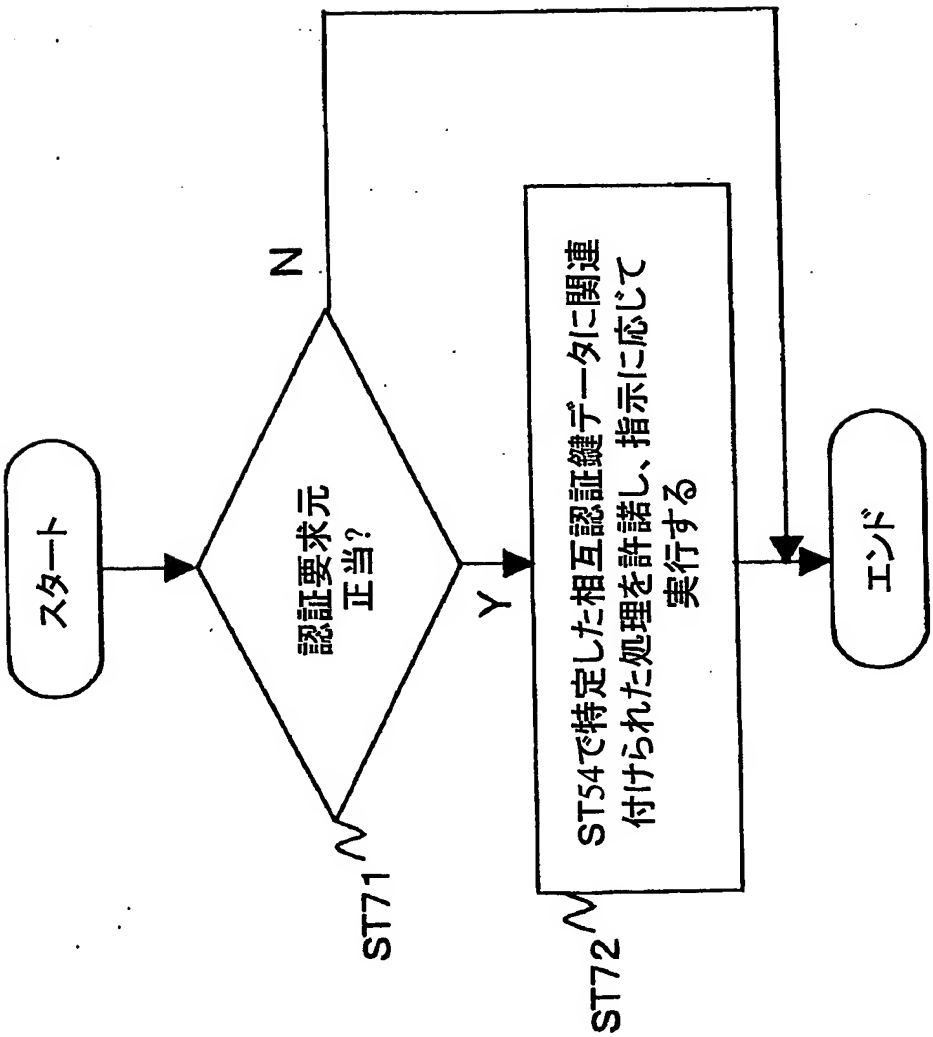

SAMユニット9a
管理装置20
(SAM管理機能部57)
縮退鍵Kbを用いてアルゴリズム2でRbを暗号化してRb'生成
ST59
Ra'', Rb'出力
ST60
縮退鍵Kaを用いてアルゴリズム2でRa'', Rb'を復号してRa, Rb生成
ST61
ST51のRaと、ST61のRaとを比較して認証
ST62
縮退鍵Kaを用いてアルゴリズム1でRbを暗号化してRb''生成
ST63
Rb''出力
ST64
縮退鍵Kbを用いてアルゴリズム1でRb''を復号してRb生成
ST65
ST58のRbと、ST65のRbとを比較して認証
ST66

FIG. 27


スタート
認証要求元
正当?
N
Y
ST71
ST54で特定した相互認証鍵データに関連
付けられた処理を許諾し、指示に応じて
実行する
ST72
エンド

符号の説明

1…通信システム

2…サーバ装置

3…ＩＣカード

4…カードＲＷ

6…ＰＣ

7…外部メモリ

8…ＳＡＭモジュール

９ａ，９ｂ…ＳＡＭユニット

１９ａ，１９ｂ…ＡＳＰサーバ装置

２０…管理装置 ５１…ＡＰ編集ツール

５２…管理ツール

５３…カードリーダ・ライタ

５４…ディスプレイ

５５…Ｉ／Ｆ

５６…操作部

５７…ＳＡＭ管理機能部

５８…カード管理機能部

６１…メモリＩ／Ｆ

６２…外部Ｉ／Ｆ

６３…メモリ

６４…認証部

６５…ＣＰＵ

７１…デフォルトカード

７２…オーナカード

７３…ユーザカード

７４…トランスポートカード

７５…ＡＰ暗号化カード

３０１…データ処理システム

３０２，３０３…データ処理装置

３０２，３１０…メモリ

３１１…認証部

３１２…暗号化部

３１３…インタフェース

３１４…ＣＰＵ

３３０…メモリ

３３１…認証部

３３２…復号部

３３３…Ｉ／Ｆ

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/11804

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/08, H04L9/10, H04L9/32, G09C1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/08, H04L9/10, H04L9/32, G09C1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2003
Kokai Jitsuyo Shinan Koho	1971-2003	Jitsuyo Shinan Toroku Koho	1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	JP 2000-332748 A (Sony Corp.), 30 November, 2000 (30.11.00), Full text & EP 1037131 A	6,8,9,10,13, 14 1-5,7,11,12
X Y	JP 2002-111658 A (Sony Corp.), 12 April, 2002 (12.04.02), Full text & EP 1176757 A	6,8,9,10,13, 14 1-5,7,11,12
X Y	JP 7-87078 A (Kabushiki Kaisha Roreru Intelligent Systems), 31 March, 1995 (31.03.95), Full text (Family: none)	6,8,9,10,13, 14 1-5,7,11,12

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 10 December, 2003 (10.12.03)	Date of mailing of the international search report 24 December, 2003 (24.12.03)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/11804

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 10-327142 A (Sony Corp.), 08 December, 1998 (08.12.98), Full text & EP 867843 A	1-5,7,11,12
X	JP 2000-332742 A (Sony Corp.), 30 November, 2000 (30.11.00), Full text & EP 1054314 A	6,8,9
A	JP 8-242224 A (Tatsuhiro MEYA), 17 September, 1996 (17.09.96), Full text (Family: none)	1-14

国際調査報告

国際出願番号　PCT／JP03／11804

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷　H04L9／08, H04L9／10, H04L9／32, G09C1／00

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷　H04L9／08, H04L9／10, H04L9／32, G09C1／00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報　1922－1996年
日本国公開実用新案公報　1971－2003年
日本国登録実用新案公報　1994－2003年
日本国実用新案登録公報　1996－2003年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP 2000－332748 A（ソニー株式会社） 2000. 11. 30, 全文 & EP 1037131 A	6, 8, 9, 10, 13, 14
Y		1-5, 7, 11, 12
X	JP 2002－111658 A（ソニー株式会社） 2002. 04. 12, 全文 & EP 1176757 A	6, 8, 9, 10, 13, 14
Y		1-5, 7, 11, 12

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
10. 12. 03	21.12.03

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	
日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	石田　信行	5M　9469
	電話番号　03－3581－1101　内線　3598	

様式PCT／ISA／210（第2ページ）（1998年7月）

国際調査報告

国際出願番号　PCT／JP03／11804

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP 7－87078 A （株式会社ローレルインテリジェントシステムズ） 1995．03．31，全文（ファミリーなし）	6, 8, 9, 10, 13, 14
Y		1-5, 7, 11, 12
Y	JP 10－327142 A（ソニー株式会社） 1998．12．08，全文 & EP 867843 A	1-5, 7, 11, 12
X	JP 2000－332742 A（ソニー株式会社） 2000．11．30，全文 & EP 1054314 A	6, 8, 9
A	JP 8－242224 A（女屋達廣） 1996．09．17，全文（ファミリーなし）	1-14